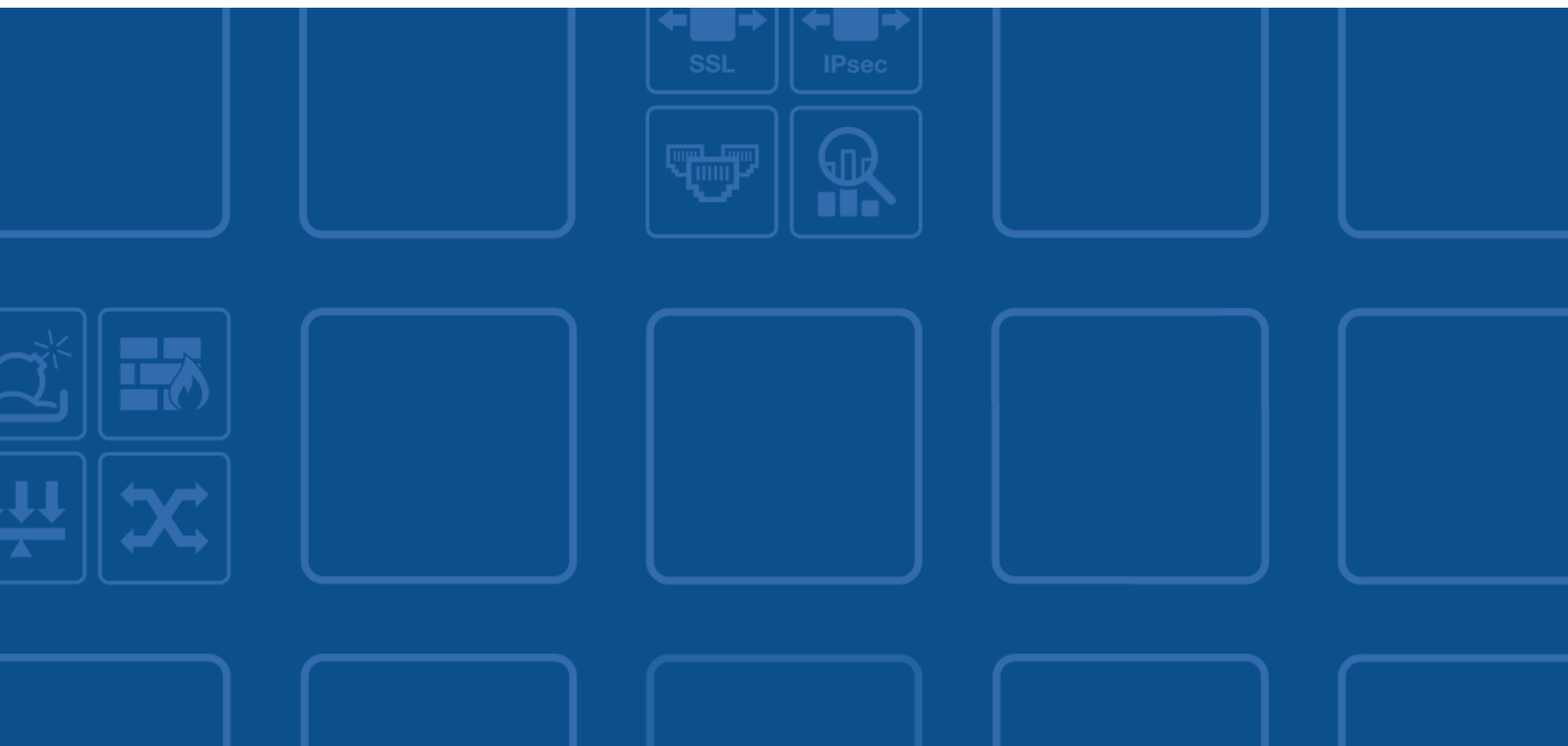
FORTINET
High Performance Network Security

FortiClient EMS - Administration Guide

VERSION 1.0.1



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July 07, 2016

FortiClient EMS 1.0.1 Administration Guide

04-101-372713-20160707

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-07-07	Initial release

Introduction

FortiClient Enterprise Management Server (FortiClient EMS) is a security management solution that enables scalable and centralized management of multiple endpoint devices (computers). FortiClient EMS provides an efficient and effective administration of endpoints running FortiClient. It provides visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.

FortiClient EMS is designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints. Some of the benefits of deploying FortiClient EMS include:

- Remotely deploying FortiClient software to Windows PCs
- Updating profiles for endpoint users regardless of access location, such as, administering antivirus, web filtering, VPN, and signature updates
- Administering FortiClient endpoint registrations, such as, accept, de-register, and block registrations
- Managing endpoints, such as, status, system, and signature information
- Identifying outdated versions of FortiClient software

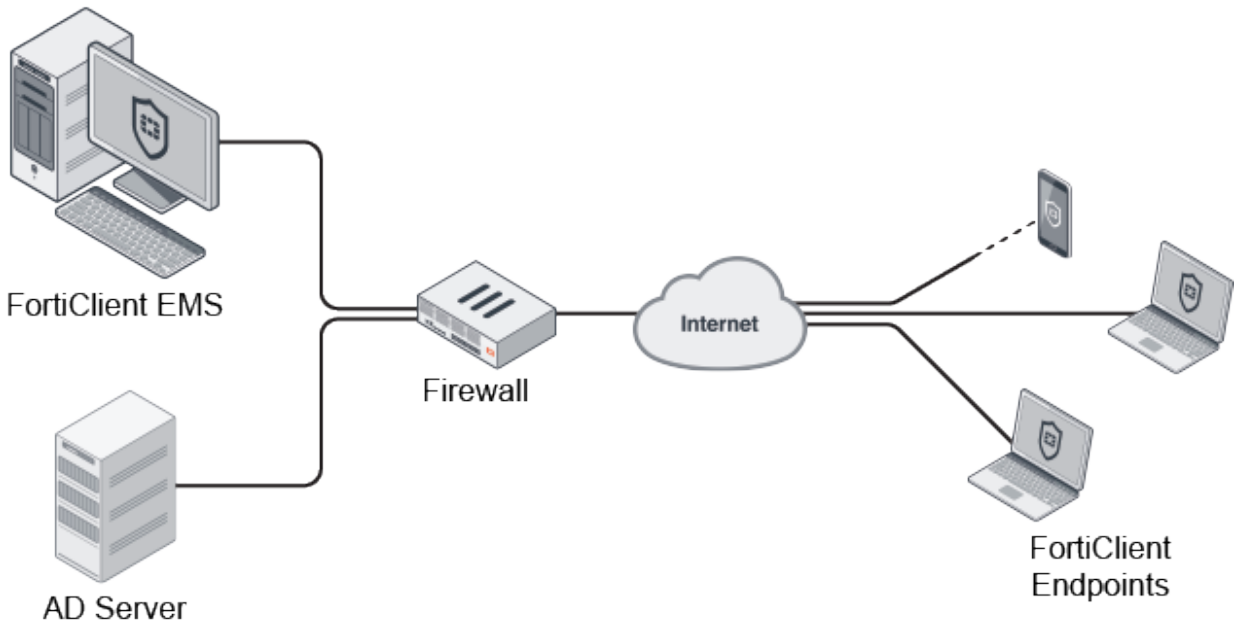
You can manage endpoint security for both Windows and Mac OS X platforms by using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view.

Components of FortiClient EMS

FortiClient EMS provides the infrastructure to install and manage FortiClient Endpoint software. FortiClient protects endpoint clients from viruses, threats, and risks. FortiClient EMS can be used to ensure clients are compliant with the organization's security profiles.

The following table lists the components of FortiClient EMS.

Component	Description
FortiClient EMS	Manages the client computers (endpoints) that connect to your network. It includes the following software: • The console software that manages security profiles and client computers. • The server software provides secure communication to and from the client computers and the console.
Database	Stores security profiles and events. The SQL database is installed as part of the FortiClient EMS installation.
FortiClient	Enforces security and protection on the client computers (endpoints). It runs on servers, desktops, and portable computers you wish to be secured. See the *FortiClient Administration Guide* on docs.fortinet.com for more information.



FortiClient EMS allows you to:

- Establish and enforce security profiles
- Manage deployment, configuration, updates, and antivirus protection reports from an integrated management console
- Obtain a consolidated view of multiple security components across all endpoint clients in your network
- Perform integrated installation of security components and set profiles

FortiClient EMS and Fortinet Endpoint Security Management

FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures a comprehensive policy administration and enforcement for an enterprise network.

Documentation

You can access the FortiClient EMS documentation from the following link: docs.fortinet.com

The FortiClient EMS documentation set includes the following documents:

- *FortiClient EMS 1.0.1 Release Notes*

  This document describes new features and enhancements in the FortiClient EMS system for the release and lists any known issues and limitations. This document also defines supported platforms and the required minimum system requirements.
- *FortiClient Enterprise Management Server - QuickStart Guide*

  This document describes how to install and begin working with the FortiClient EMS system. It provides instructions on installation, deployment, and also includes a high-level task flow for using the FortiClient EMS system.

- *FortiClient EMS 1.0.1 Administration Guide*
  This document describes how to set up FortiClient EMS and use it to manage FortiClient endpoints. It includes information on how to configure multiple endpoints, configure and manage profiles for the endpoints, and view and monitor the FortiClient endpoint profile status.

What's New in FortiClient EMS 1.0.1

The new features in FortiClient EMS 1.0.1 include the following:

What was New in FortiClient 1.0.1:

Assign FortiClient Telemetry Gateway IP List to Endpoints

Instead of managing and monitoring endpoints from FortiGate and FortiClient EMS, this feature de-couples the FortiGate IP List from the rest of the profile. This allows users to manage and monitor endpoints only using FortiClient EMS.

The user selects an Endpoint Profile and assigns a FortiClient Telemetry Gateway IP List. Then, deploys by assigning the FortiClient Telemetry Gateway IP List to an Endpoint Profile. After deployment, the endpoint will register to a FortiGate based on the FortiClient Telemetry Gateway IP List.

Users can assign FortiClient Telemetry Gateway IP Lists to endpoints (even if the endpoint is already registered to a FortiGate) and update FortiGate IPs as required.

Auto-Sync FortiClient Profiles with FortiGate

Users can manage profile configurations from one place while using FortiClient EMS to manage client deployment. Users can auto-sync profile changes to FortiClient EMS once its been modified on the FortiGate.

It will only deploy to endpoints if they are registered to the EMS.

CA Certificates imported from FortiGates

FortiClient EMS can pull CA certificates from FortiGates through a protocol that does not need authentication (SNMP). These CA certificates are pulled from various FortiGates and can be grouped and/or managed. Users can push these CA certificate groups to selected FortiClient endpoints. Thereupon, FortiClient will download and install them into the endpoint's certificate store as a trusted certificate.

Deploy a FortiClient Upgrade from EMS

You can deploy a FortiClient software update from EMS. A prompt will appear in the FortiClient endpoint when an installer package is requested to be deployed.

Email Alert Notifications

You can add an option to setup a SMTP server to enable an Alert for Endpoint Events. When an alert is triggered, an email notification will be sent.

Host names and License Updates

When you update your license information, FortiClient EMS will update the serial number of the FortiClient Telemetry server once. You are able to change the EMS host name in the settings dialog.

Vulnerability Scan Settings and Summary Chart

Administrators are able configure the Vulnerability Scan Settings for each endpoint profile.

The Vulnerability Scan Summary Chart provides a centralized vulnerability summary for all monitored endpoints. Administrators are able to get a good idea of high risk hosts and critical vulnerabilities that exist on endpoints. It also provides links on how to fix or repair the vulnerabilities.

FortiGate Integration with FortiClient EMS

To integrate FortiGate with FortiClient EMS, users must set up a FortiClient Endpoint Compliance in the FortiGate and import the profile to FortiClient EMS for deployment. Profiles created in EMS do not support NAC.

If users want to update profiles after deployment, the profile must be updated in FortiGate, not FortiClient EMS.

FortiGate Managed Endpoints Summary Chart

This chart indicates how many clients are registered to specific FortiGates.It provides an overview of the FortiGate Managed Endpoint registration status.

LDAP Integration for Administrator Login

LDAP integration implementation allows LDAP users to login to FortiClient EMS as an administrator.

The list of LDAP users is derived from the server on which FortiClient EMS is installed. If you want to add more LDAP users, you must add them to the server.

License Expiration Notification

When the FortiClient EMS License is near expiration, a pop-up message will appear:

- When 60 days are left
- When 30 days are left
- Upon every login when there are less than 30 days left

The same license expiration notification will be shown (bell icon) in the top banner.

MSSQL Server Enterprise Edition

FortiClient uses a pre-installed MSSQL server to improve scaling. You can choose to install the MSSQL Enterprise using its default settings, or you can use command line options to configure the MSSQL Enterprise settings. For the description of commands, go to Installation.

Purchased Licenses

Instead of stacking licenses, you can now specify the number of FortiClient EMS licenses and the duration of use at the time of purchase.

Updated Trial License

When you install FortiClient EMS, the free trial license is enabled by default. The free trial license supports 10 FortiClient endpoints. FortiClient EMS consumes one license count for each managed FortiClient device.

For a free 60 day trial, please contact a sales representative.

Overview

This section provides an overview of how to:

- Install and configure FortiClient EMS.
- Discover endpoint devices and deploy FortiClient
- Monitor and update endpoint devices

Installing and configuring FortiClient EMS

Before installing FortiClient EMS, it is recommended that you read the *FortiClient EMS Release Notes* and the *FortiClient Enterprise Management Server - QuickStart Guide* available on docs.fortinet.com to become familiar with relevant software components and other important information about the product.

Following is an overview of how to install and configure FortiClient EMS.

1. Prepare for the FortiClient EMS installation. See Required services and ports on page 18.
2. Install FortiClient EMS. See Installing FortiClient EMS on page 23.
3. Log into FortiClient EMS. See Logging into FortiClient EMS on page 24.
4. License FortiClient EMS. See Installation on page 23.
5. Configure FortiClient EMS settings. See Settings on page 30.
6. Configure user accounts and permissions. See User Management on page 38.

Deploying FortiClient to endpoints

Following is an overview of how to discover endpoint devices and deploy FortiClient on the endpoint devices from FortiClient EMS.

1. Discover endpoint devices. See Adding Endpoints on page 44.
2. Add FortiClient installers to FortiClient EMS, and specify what FortiClient features to install. See Adding installers on page 51.
3. Configure profiles to select the FortiClient installer and specify settings for the features that it will install. See Configuring profiles on page 55.
4. Prepare domains and workgroups for deployment. See Preparing the AD Server for Deployment on page 74.
5. Assign profiles to domains and workgroups to deploy FortiClient on endpoints. See Assigning profiles to endpoints on page 56.
6. Create and assign FortiClient Telemetry Gateway IP Lists to endpoints. See Creating FortiClient Telemetry Gateway IP Lists on page 72 and Assigning FortiClient Telemetry Gateway IP Lists to endpoints on page 73.

Integrating FortiGate with FortiClient EMS

To integrate FortiGate with FortiClient EMS, users must set up a FortiClient Endpoint Compliance in FortiGate and import the profile to FortiClient EMS for deployment. Profiles created in EMS do not support NAC.

FortiClient profiles created by using FortiGate contain compliance rules to support NAC, and they might contain configuration information, depending on the non-compliance setting in the FortiClient profile.

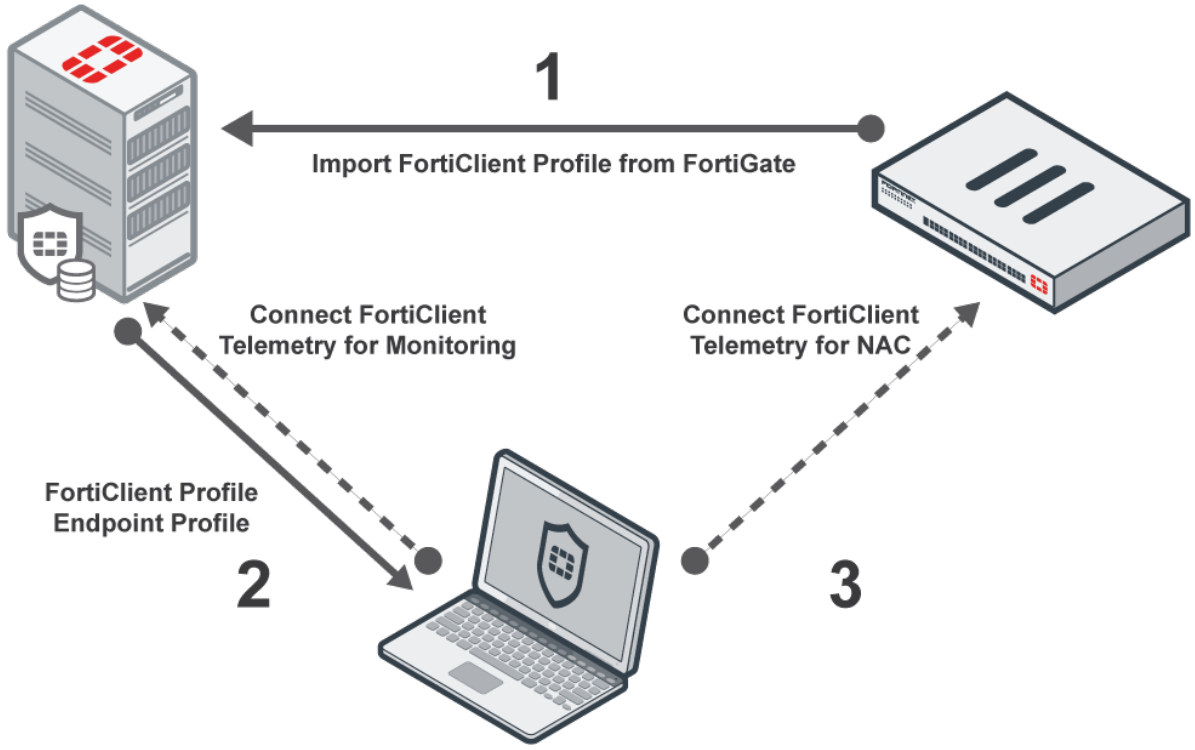
When non-compliance is set to *Block or Warn*, the FortiClient profile contains compliance rules, but no configuration information. When non-compliance is set to *Auto-Update*, the FortiClient profile contains compliance rules and some configuration information. For more information about FortiClient profiles and compliance rules, see the *FortiOS Handbook*.

How FortiGate integrates with FortiClient EMS depends on the non-compliance setting in the FortiClient profile:

Block or Warn:

When non-compliance is set to *Block or Warn*, you can create an endpoint profile in EMS and assign the profile to endpoints. The profile from EMS is in addition to the FortiClient profile from FortiGate.

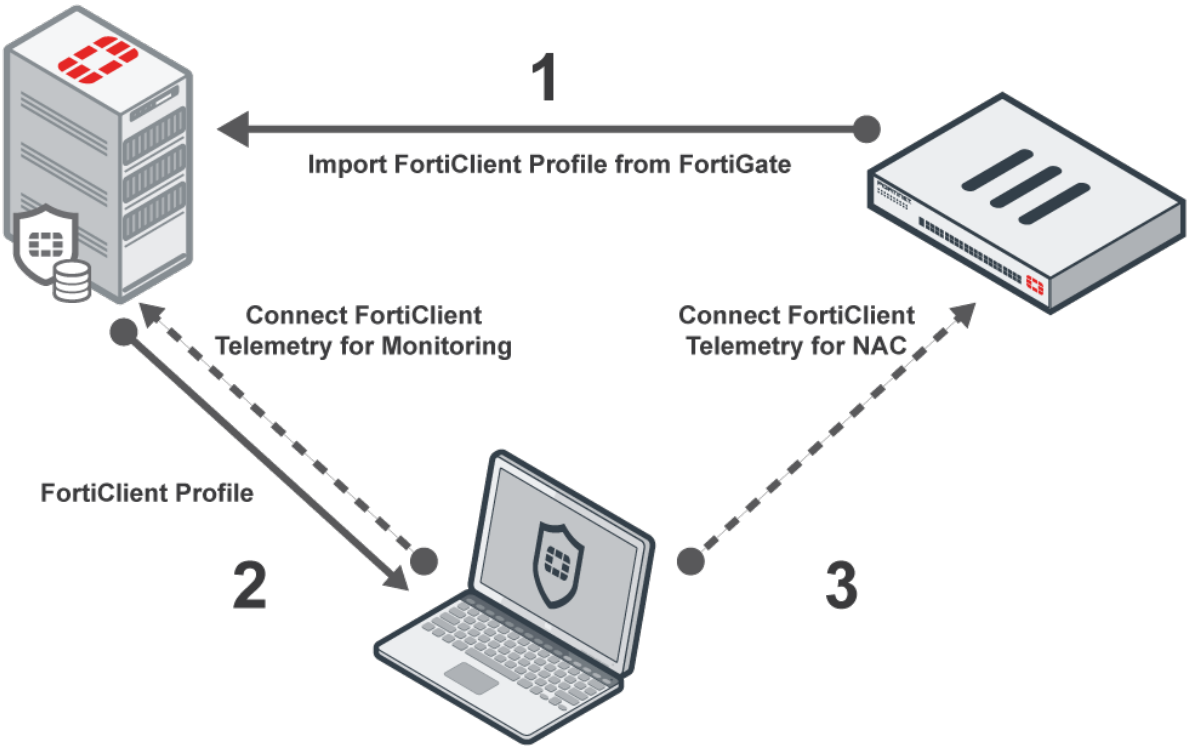
1. Using a FortiGate running 5.4.1 and later, create a FortiClient profile.
2. On FortiClient EMS, import the FortiClient profile.
   a. Import the FortiClient profile and review the compliance rules.
   b. Create an endpoint profile that enables the options required by the compliance rules, such as AntiVirus and so on.
   c. Create a FortiClient Telemetry Gateway IP List for the FortiGate.
   d. Assign an installer to the profile.
   e. Assign the FortiClient Telemetry Gateway IP List to endpoints.
      If the installer comes with the FortiGate IP list, endpoints will be assigned automatically.
   f. Assign the FortiClient profile to the endpoints. This will deploy the installer and compliance rules to endpoints. The endpoints connect FortiClient Telemetry to the FortiGate.
   g. Assign the endpoint profile from EMS to the endpoints. This will deploy the configuration to endpoints.
3. Use FortiClient EMS to monitor endpoints.
4. On the FortiGate update the profile as needed. Changes are automatically pushed to the endpoints.



Auto-Update

When non-compliance is set to *Auto-Update*, you can assign only the FortiClient profile from FortiGate to endpoints. The FortiClient profile contains the compliance rules, but no configuration.

1. Using a FortiGate running 5.4.1 and later, create a FortiClient profile.
2. On FortiClient EMS, import the FortiClient profile.
   a. Import the FortiClient profile.
   b. Create a FortiClient Telemetry Gateway IP List for the FortiGate.
   c. Assign an installer to the profile.
   d. Assign the FortiClient Telemetry Gateway IP List to endpoints.
      If the installer comes with the FortiGate IP list, endpoints will be assigned automatically.
   e. Assign the FortiClient profile to the endpoints. This will deploy the installer. The endpoints register to the FortiGate
3. Use FortiClient EMS to monitor endpoints.
4. On the FortiGate update the profile as needed. Changes are automatically pushed to the endpoints.



Managing and updating endpoint devices

Following is an overview of how to monitor endpoint devices.

1. Monitor endpoint status. See Viewing endpoint status on page 49.
2. Monitor FortiClient EMS status. See Endpoint status on page 49.
3. Update profiles to update FortiClient on endpoint devices. See Editing profiles on page 57.

Requirements and Dependencies

You can install and use FortiClient EMS as a standalone product on an active directory server or a standalone Windows machine. Requirements for installation and operation vary in relation to the presence of other software on the server and according to how you use FortiClient EMS.

Required services and ports

You must ensure that required ports and services are enabled for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with clients and servers running associated applications.

Communication	Service	Protocol	Port
FortiClient endpoint	File transfers	TCP	8013 (default)
Computer browser service • Computer browser service is not needed if an Active Directory is used or clients can manually register to EMS.	Enabled		
Samba (SMB) service • During FortiClient deployment, endpoints may connect to the FortiClient EMS server using the SMB service.	Enabled		445
Distributed Computing Environment / Remote Procedure Calls (DCE- RPC) • The FortiClient EMS server connects to the endpoints using RPC for FortiClient deployment.	Enabled		135
Active Directory server connection	When used as a default con-nection		389
Apache	HTTPS	TCP	443, 10443
SQL server			

Ensure that the Computer Browser Service is running. On Windows Server 2012 R2, the service is disabled by default. If this service is not active, FortiClient EMS cannot detect computers on the same network, even if they are available.

Management Capacity

The EMS is intended for use by enterprises. It has the capacity to manage a large number of endpoints. The following are suggested EMS host system hardware configurations, depending on the number of endpoints being managed.

Suggested minimum EMS system hardware

Max number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
10, 000	2	4	default
20, 000	4	8	default
30, 000	4	8	120 seconds
40, 000	4	8	120 seconds
50, 000	4	8	120 seconds

For the purpose of this table, an Intel i5 processor with two cores and two threads per core will be considered to have 4 virtual CPUs. An Intel i3 processor with two cores and one thread per core has two virtual CPUs.

Each registered FortiClient sends a short keep alive message to the EMS at a regular interval. The keep alive message carries various update information from the client to the EMS. If a modification or change is made on the EMS, it sends it to the clients in the keep alive reply.

The default keep alive interval in FortiOS 5.2 is 120 seconds. It is 60 seconds by default in the EMS. To change the keep alive interval, go to *View* > *Settings* and enter the appropriate time in the *Keep Alive Interval* field

Server readiness checklist for installation

Use the following checklist to prepare your server for installation, after you verify that the server meets the requirements described in Required services and ports on page 18".

Checklist	Readiness Factor
	Temporarily disable security applications. You must temporarily disable any antivirus software on the target server before you install FortiClient EMS. Installation might be slow or disrupted while these programs are active. Note that a server might be vulnerable to attack when you uninstall or disable security applications.

Checklist	Readiness Factor
	Carefully consider the date and time settings that you apply to your server.
	Confirm that required services and ports are enabled and available for use by FortiClient EMS.
	Ensure that no conflict exists with Port 443 and 10443 for Apache service to function properly.

Licenses

This section describes the licensing options available for FortiClient EMS. It provides information about the number of supported FortiClient endpoints for each type of license to help you determine which license best suits your needs. This section provides the licensing information for FortiClient EMS.

Description of licenses for FortiClient EMS

FortiClient EMS supports the following types of licenses:

- Free trial license
- Purchased license

Free trial license

When you install FortiClient EMS, the free trial license is enabled by default. The free trial license supports 10 FortiClient endpoints. FortiClient EMS consumes one license count for each managed FortiClient device.

For a free 60 day trial, please contact a sales representative.

Purchased license

Each purchased license allows management of one FortiClient endpoint. You will need to purchase a minimum of 100 endpoints and you have an option to have this EMS license for a maximum three year term. You can specify the number of endpoints and the duration of term at the time of purchase.

You can use a licensed EMS to deploy, provision, and manage FortiClient endpoints. However, if have a FortiGate in your network, you can buy an Add-On FortiGate End-point license to enforce Endpoint Compliance on the Firewall while endpoints are being managed by EMS. Using FortiGate with EMS is optional.

Licensing FortiClient EMS

The following will describe how to license FortiClient EMS.

1. Visit forti.net/Reseller to find a Reseller.

   Once you purchase FortiClient EMS, you will receive the *FortiClient Host Security License Certificate* via email. This email contains the *Certificate Number* that will be used to obtain the FortiClient EMS License.

2. Login to the Fortinet Support site.
   a. Click *Register and Renew*.
   b. Enter the *Certificate Number*. This is the number you received in the FortiClient Host Security License Certificate email.

If you have not already registered an EMS device, you will be prompted to do so. This will require obtaining the *Hardware ID* from FortiClient EMS. You can obtain the *Hardware ID* by clicking the *Upgrade* link located in the *FortiClient EMS Dashboard*.

c. Enter the *Hardware ID*.
d. Enter the *Fortinet Partner Reseller*.
e. Read, verify and agree to the *Terms and Conditions* of the service.
f. Verify the Product Entitlement List for your recent FortiClient EMS purchase. Check the *By accepting these terms...* checkbox. Then, click *Confirm*. The license file will now be available to use with your FortiClient EMS installation.
g. Click *Finish*.
h. From your *Products List*, select FortiClient EMS.
i. From the left panel, select *License and Key*.
j. From the *Available Keys List*, select the FortiClient EMS entry. Then, click *Get the License File*.
k. From FortiClient *EMS Dashboard* > *Upgrade*, click *Browse*.
l. Select the license file and *Upload File*. You have successfully licensed FortiClient EMS.

If you need to renew your license or make changes to your requirements, please contact Fortinet Support.

Upgrading the FortiClient EMS license

To upgrade the FortiClient EMS license:

1. Go to *View* > *Upgrade License*. The *Add FortiClient EMS License* pane is displayed.
2. Click *Browse*, locate the license key file, and click *Upload File*.

Licenses for component applications

Common services or applications do not require a license. See the *FortiClient Enterprise Management Server - QuickStart Guide* for more information about the common components.

During the installation of common services required for FortiClient EMS, you are not asked for license information.

Help with Licensing

For licensing issues with FortiClient EMS, contact the licensing team at Fortinet Technical Assistance Center (TAC):

- Phone: +1-866-648-4638
- Technical support: support.fortinet.com/

Installation

Before you install and license FortiClient EMS on a server, ensure you have:

- Reviewed Description of licenses for FortiClient EMS on page 21
- Met the requirements listed in the Required services and ports on page 18
- Completed the Server readiness checklist for installation on page 19
- Logged into the server as administrator. The administrator user account is equivalent to a Windows administrator account and provides access to all common services, FortiClient EMS, and other application tasks. You can use this account to initially log in to the server and to create other user accounts for normal day-to-day use of the applications.

It is recommended that you install FortiClient EMS on a dedicated server in a controlled environment. Installing other software applications can interfere with the normal operation of FortiClient EMS.

Installing FortiClient EMS

Installing and licensing FortiClient EMS requires the following steps:

1. Be aware of software dependencies.
2. Obtain or locate the FortiClient EMS installation program.
3. Run the FortiClient EMS installation program.

Obtaining the FortiClient EMS installation program

FortiClient EMS is available for download from the following locations:

- Fortinet Support website (support.fortinet.com)
- Sales representative

Running the FortiClient EMS installation program

To install FortiClient EMS:

1. Double-click the downloaded installation file for FortiClient EMS. The installation wizard starts.

If you are not logged into the server as an administrator, right-click the installation file and select *Run as administrator*.

2. Follow the installation wizard instructions.
   In the License terms and agreement window: Select *I agree to the license terms and conditions* if you agree with the license terms and conditions. If you do not agree, the installation process stops.
3. Click *Install*.

The applications that will be installed appear. The FortiClient EMS installation package includes the following applications: *FortiClient EMS, Microsoft SQL Server 2014 Express Edition, Apache HTTP server, and Python*. The installation setup process begins.

4. Continue following the installation wizard instructions.
   After the program has installed, the *Setup Successful* window appears.
5. Click *Close*.
   A desktop icon is created, which opens the FortiClient EMS application home page.
6. Re-enable any antivirus applications that you temporarily disabled.

Existing services running on default FortiClient EMS ports

In cases where there are pre-existing services running on default FortiClient EMS ports, you can specify another port to be used using the CLI to run the installer.

Use the following commands:

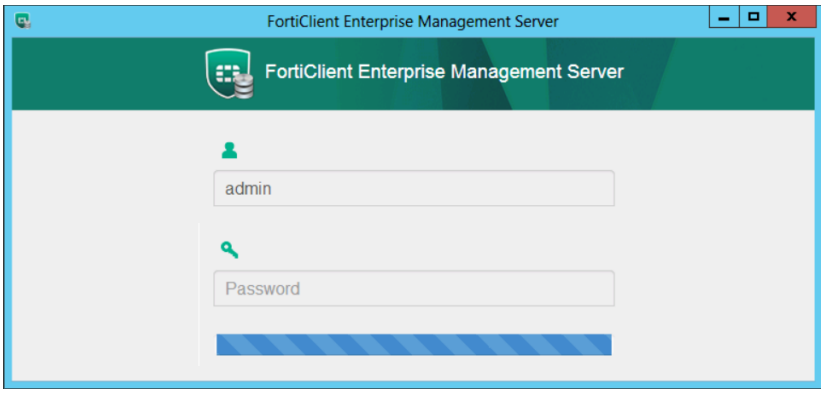
Command	Description
`ClientDownloadPort`	The port FortiClient will be downloaded from FortiClient EMS.
`RemoteManagementPort`	The port that will be used for EMS administration.
Example: `FortiClientEnterpriseManagement_1.0.0.6401_interim_x64.exe RemoteManagementPort=10553`	

Logging into FortiClient EMS

FortiClient EMS runs as a service on Windows computers.

To open FortiClient EMS:

1. Double-click the FortiClient EMS icon, or select *Start* > *All Programs* > *FortiClient Enterprise Management Server* to start the application.
2. Log in by using the default admin account. Enter `admin` for user name, and leave the password field empty. Click *Sign in*. The FortiClient EMS application opens.



The client automatically closes if it is idle for 30 minutes.

3. Add a password to the administrator account by going to *View* > *User Management*. See also Configuring user management on page 38.
4. To exit the application, click *Admin* > *Logout* from the toolbar.

Accessing FortiClient EMS remotely

FortiClient EMS can be accessed using a web browser in lieu of the GUI.

- To access the EMS from the EMS server, visit `https://localhost`.
- To access the server remotely, use the server's hostname: `https://<server_name>`.

Ensure you can access the device remotely. This can be achieved by adding it into a DNS entry, or by adding it to the Windows hosts file. You may have to modify the Windows Firewall rules to allow the connection.

You will need to have *View* > *Settings* > *Server Settings* > *Remote Administration HTTPS Access* enabled on the FortiClient EMS to access the server's hostname.

Uninstalling FortiClient EMS

Use the *Programs and Features* pane of the Control Panel in Microsoft Windows to uninstall FortiClient EMS.

FortiClient EMS installs the following dependencies. If they are not being used by other applications on the same computer, they can be uninstalled manually after the EMS has been removed.

- Microsoft ODBC Driver 11 for SQL Server
- Microsoft SQL Server 2008 Setup Support Files
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2014 (64-bit)
- Microsoft SQL Server 2014 Setup (English)
- Microsoft SQL Server 2014 Transact-SQL ScriptDom
- Microsoft Visual C++ 2010 x64 Redistributable – 10.0
- Microsoft Visual C++ 2010 x86 Redistributable – 10.0

- Microsoft Visual C++ 2013 x86 Redistributable – 12.0
- Microsoft VSS Writer for SQL Server 2014
- SQL Server Browser for SQL Server 2014

To uninstall FortiClient EMS:

1. Select *Start* > *Control Panel* > *Programs* > *Uninstall a program*.
2. Select *FortiClient Enterprise Management Server*, and click *Uninstall*.
3. Follow the uninstallation wizard prompts.

GUI

Navigating the FortiClient EMS Interface

FortiClient EMS offers a centralized view of managing FortiClient endpoints and allows you to define and make endpoint security profile changes.

The application provides views or panes in which you can manage endpoints and profiles, such as domain and workgroup, endpoint profile, and content pane views. You can switch between these views according to your needs. The user interface is a graphical summary of important security information about the endpoint clients in your organization.

Banner

Option	Description
License Type	Displays current license information.
Bell icon	Clicking the Bell icon displays all Alerts.
View	View and configure the following: • Upgrade License • Software Manager • User Management • CA Certificate Management • Database Management • View Logs • Settings
Help	View the following: • Technical Documentation • How-To Videos • Forums • Getting Started • About
Admin	Logout of FortiClient EMS.

Left Pane

The left navigation pane is used to display content in the right content pane.

Option	Description
Dashboard	Display a dashboard of information about all managed FortiClient endpoints.
Vulnerability Scan	The Vulnerability Scan Summary Chart provides a centralized vulnerability summary for all monitored endpoints. Administrators are able to get a good idea of high risk hosts and critical vulnerabilities existing on endpoints. It also provides links on how to fix or repair the vulnerabilities. When you click on a circle, it drills down the vulnerability details
Endpoints	Add and manage endpoints. You can add and manage endpoints from domains and from workgroups.
Endpoint Profiles	Create and assign profiles as well as manage profile updates.
FortiClient Telemetry Gateway IP Lists	Create and assign FortiClient Telemetry Gateway IP Lists as well as manage IP list updates.

Right Pane

The right content pane displays the user interface controls that correspond to the selection you make in the left navigation pane. The status and menu icons on the top-right display controls that you can use to configure additional settings for user management and each individual endpoint.

To view the dashboard:

1. Click the *Dashboard* on the left pane. A summary of the status of the endpoints is displayed.
2. Click any of the pie charts or any row in the table to view more details about the summarized endpoints.
3. Click any of the displayed endpoints to view more details about the endpoint.

Charts

In the right pane, there are a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each of the charts are links. You can click any section of the pie charts or any row in the table to display more details.

Option	Description
Client Stats	Statistics of Clients in use.
FortiGate Managed Endpoints Summary Chart	This chart indicates how many clients are registered to which FortiGates. It provides an overview of the FortiGate Managed Endpoint status.
Devices by OS	This chart indicates how many clients are registered to and using which OS.

Option	Description
Event Summary	Summary of events • Endpoints with Out-of-date Protection • Endpoints with Out-of-sync Profiles • Endpoints with Pending Software Updates • Errors or Warnings (last 7 days) • Inactive Endpoints (last 30 days) • Unprotected Clients
Installed FortiClient Version Summary	Percentage of FortiClient versions used.
Vulnerability Scan Chart	The chart provides a centralized vulnerability summary for all monitored endpoints, and an overall idea of high risk hosts and critical vulnerabilities existing on the endpoints.

Settings

This section describes FortiClient EMS server settings and log settings. It also describes how to import CA certificates as well as back up and restore the database.

FortiClient EMS Settings

Server Settings

FortiClient EMS installs with a default IP address and port configured. You can change the IP address and port, and configure other server settings for FortiClient EMS.

To configure server settings:

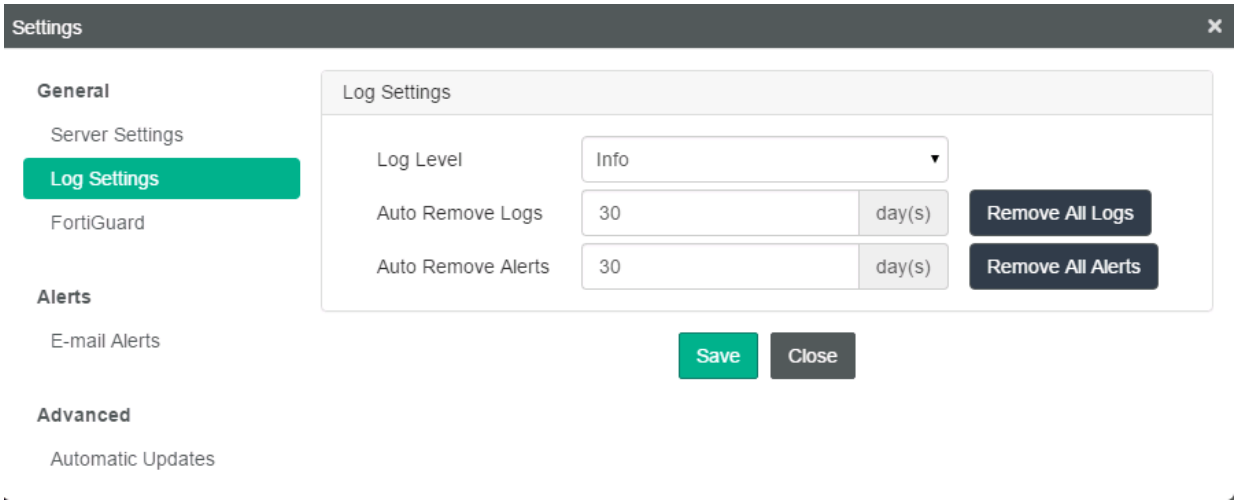
1. Go to *View* > *Settings*.
2. Select *Server Settings*, and configure the options. For a description of the options, see the Server Settings Tab on page 33.
3. Select *Save*.

Log settings

You can specify what level of log messages to capture in the logs for FortiClient EMS. You can also specify when to automatically delete logs and alerts.

To configure log settings:

1. Go to *View* > *Settings*.
2. Under *Log Settings*, configure the options. For a description of the options, see Log Settings Tab on page 34.
3. Select *Save*.

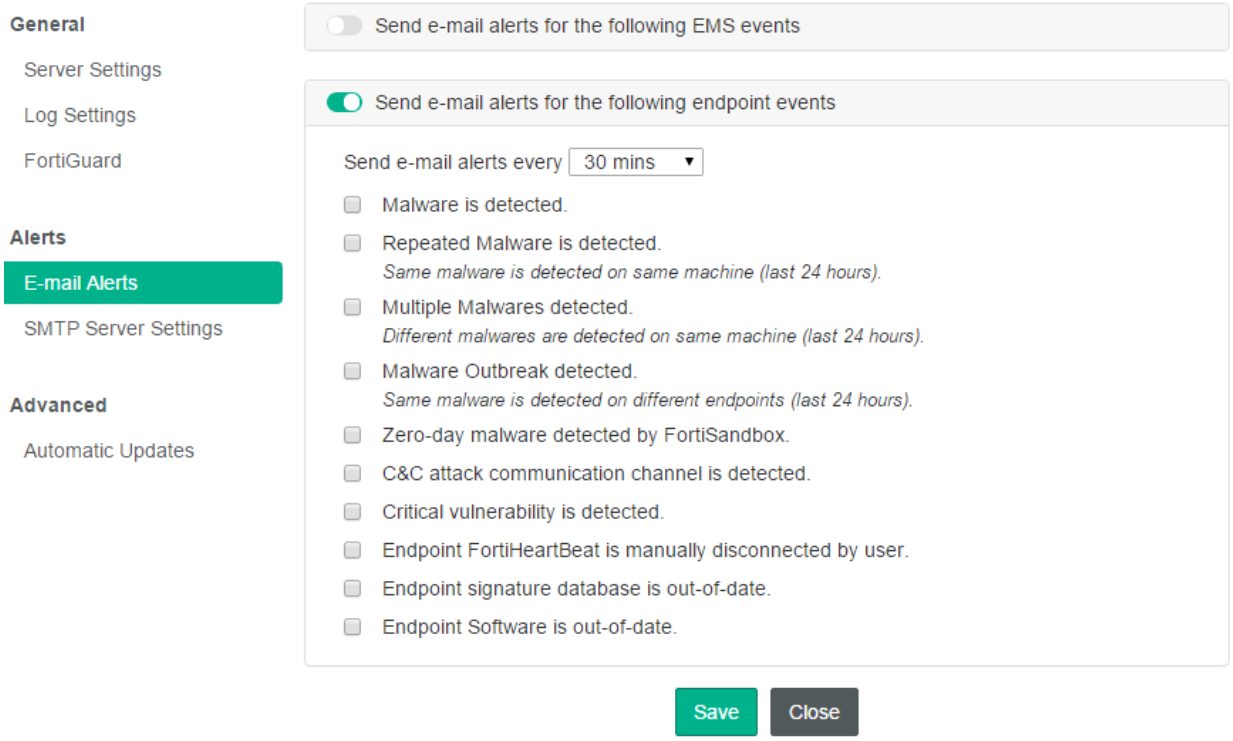


Email Alert Settings

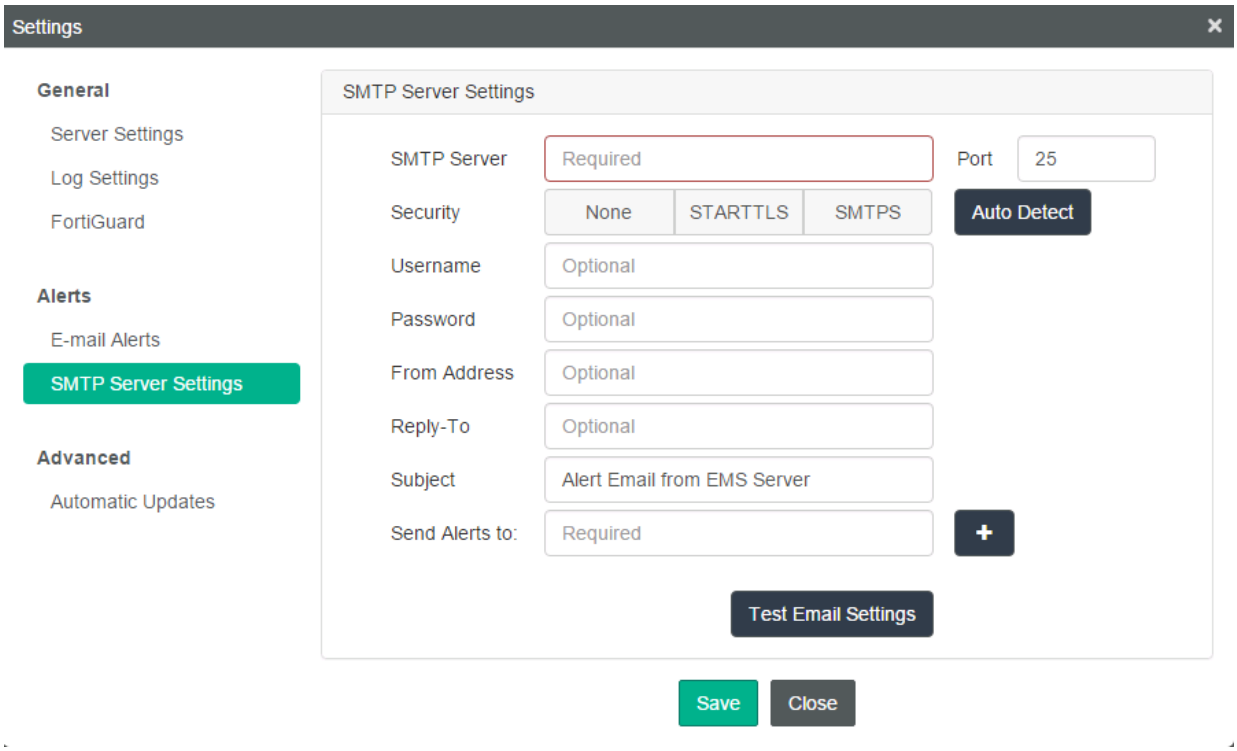
You can add an option to setup a SMTP server to enable an Alert for Endpoint Events. When an alert is triggered, an email notification will be sent.

To configure Email Alerts and a SMTP server

1. Go to *Settings* > *Alerts* > *Email Alerts*
2. Enable *Send e-mail alerts for the following endpoint events*.
3. Select the *Alert* types you would like to receive an email notification for.



4. Click *Save*.
5. If you have not already set up a SMTP Server, the GUI will automatically prompt you to configure the *SMTP Server Settings* information. See the Configuration references on page 33.



6. Click *Save*.

Importing certificates

You can import CA certificates into FortiClient EMS.

To import certificates:

1. Go to *View* > *CA Certificate Management*.
2. Select *Import*.
3. In the *Certificate Upload* window, select either:
   a. *Manual Upload*: If you select this option, click *Browse* to locate the certificate.
   b. *Import from FortiGate*: If you select this option, you will be require to enter the following information:

Server IP/Hostname	Enter the server P/Hostname in the following format: `<ip address> : <port>`.
VDOM	Enter the VDOM.
Username	Enter the username.
Password	Enter the password.

4. Click *Import* to import the certificate.

Backing up and restoring the database

You can back up and restore the FortiClient EMS database.

To back up the database:

1. Go to *View* > *Database Management*. The Database Operations pane is appears.
2. Select *Backup Database*.
   When the database backup is complete, Windows Explorer is appears with the database backup file selected.

To restore the database:

1. Go to *View* > *Database Management*. The Database Operations pane is displayed.
2. Select the *Restore* tab.
3. Select *Browse*, and select the database backup file.
4. Select *Restore Database*.
   When the database is restored, a message appears. The message instructs you to wait for the restored database to reload.
5. Wait for the restored database to be reloaded.

Configuration references

This section contains descriptions of the fields used to configure FortiClient EMS.

Server Settings Tab

Following is a description of the fields on the *View* > *Settings* > *Server Settings* tab.

Option	Description
Host Name	Displays the Host Name for the FortiClient EMS server.
Listen on IP Addresses	Displays the IP addresses for the FortiClient EMS server. FortiClient will register to the FortiClient EMS on the specified IP address.
Listen on Port	Displays the default port for the FortiClient EMS server. You can change the port by typing a new port number. FortiClient will register by using the specified port number.
EMS has a FQDN	Turn on to specify a fully qualified domain name (FQDN) for the FortiClient EMS server.

Option	Description
EMS FQDN	Displayed when *EMS has a FQDN* is turned on. Type the FQDN for the FortiClient EMS server. FortiClient can register by using either the specified IP address in the *Listen on IP Addresses* option or the specified FQDN.
FortiClient Telemetry Connection Key	Add the FortiClient Telemetry Connection Key for FortiClient EMS. FortiClient must provide this key during registration. There is no key by default.
Confirm Key	Add the registration key for FortiClient EMS again to confirm the key.
Keep Alive Interval	Each registered FortiClient sends a short keep-alive message to FortiClient EMS at the specified interval.
License Timeout	A license seat is consumed by each registered FortiClient. If a FortiClient unregisters from FortiClient EMS, the license seat is retained in anticipation that the FortiClient will re-register. The registration record is deleted if the FortiClient does not re-register within the given timeout.
DHCP Onnet/Offnet	Enable to monitor endpoints that are within the company network (on-net). Endpoints that register to FortiClient EMS from outside of the company network are considered off-net.
Remote administration/HTTS Access	Specify settings for remote administration access to FortiClient EMS. Turn remote HTTPS access to FortiClient EMS console on and off. When enabled, administrators can use a browser and HTTPS to log into the FortiClient EMS console. When disabled, administrators can only log into FortiClient EMS console on the server.
Custom host names	Available when *HTTPS Access* is turned on. Displays the pre-defined host name of the server on which FortiClient EMS is installed. You can customize the host name. When you change the host name, the web server restarts.
Scan local workgroups	Turn on to enable FortiClient EMS to automatically scan workgroups on the network to discover endpoint devices in the workgroups.
FortiClient download URL	FortiClient installers created on FortiClient EMS will be made available for download at the URL.
Open port 10443 in Windows Firewall	Turn on to open port 10443, and turn off to close port 10443. Port 10443 is used to download FortiClient.

Log Settings Tab

Following is a description of the fields on the *View* > *Settings* > *Log Settings* tab.

Option	Description
Log level	Select the level of messages to include in FortiClient EMS logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiClient EMS logs.
Auto Remove Logs	Type the number of days that you want to store logs. For example, if you type 30, logs will be stored for 30 days. Any logs older than 30 days are automatically deleted.
Remove All Logs	Click to immediately delete all FortiClient EMS logs.
Auto Remove Alerts	Type the number of days that you want to keep alerts. For example, if you type 30, alerts will be kept for 30 days. Any alerts older than 30 days are automatically deleted.
Remove All Alerts	Click to immediately delete all FortiClient EMS alerts.

FortiGuard Tab

FortiClient EMS regularly connects to FortiGuard to determine the current versions of FortiClient software and signatures that are available. The information is compared to the update information provided by each registered FortiClient endpoint. A summary of outdated registered endpoints is available on the FortiClient EMS dashboard.

Following is a description of the fields on the *View* > *Settings* > *FortiGuard* tab.

Option	Description
Use FortiManager for client software/signature update	Turn on to use FortiManager for updating FortiClient software or signatures. You must specify the IP address or host name for FortiManager as well as the port number.
Use proxy for updates	Turn on to specify a proxy for updates to FortiClient software.

To configure FortiManager for use by FortiClient on each endpoint, see Profile references on page 57.

Endpoint Settings

Following is a description of the fields on the *View* > *Settings* > *Endpoint Settings* tab.

Option	Description
Automatically upload user avatars to FortiClient EMS	When the automatic user avatar upload feature is enabled, FortiClient will upload user avatars to all FortiGates, FortiAnalyzers, and EMS servers it is registered to.

SMTP Server Settings

Following is a description of the fields on the *View* > *Settings* > *Alerts* > *Enable send an email for the following endpoint events* > *SMTP Server Settings*. You will need to enable *Enable send an email for the following endpoint events* to show the SMTP Server Settings.

Option	Description
SMTP Server	Enter SMTP Server.
Port	Enter Port number.
Security	Select either *None*, *STARTTLS*, or *SMTPS* for the security type.
Username	Enter Username.
Password	Enter Password.
From Address	Enter From Address.
Reply-To	Enter Reply Address.
Subject	Subject of the sent e-mail alert.
Send Alerts to	Enter email address(es) to send Alerts to.
Test Email Settings	Click the button to test the Email Settings.

Email Alerts

Following is a description of the field on the *View* > *Settings* > *Alerts* > *Email Alerts* > *Send e-mails alerts for the following EMS events*.

Option	Description
Notify when new EMS versions are available for deployment	New EMS versions are available.
Notify when new FortiClient versions are available for deployment	New FortiClient versions available for deployment.
Notify when EMS license is expiring or expired.	Expiring or expired EMS license.
Notify when EMS fails to sync with LDAP domain(s).	EMS does not sync with LDAP domains.

Option	Description
Notify when EMS fails to sync Auto-sync enabled profile(s)	EMS does not sync with Auto-sync enabled profiles.

Following is a description of the fields on the *View* > *Settings* > *Alerts* > *Email Alerts* > *Send e-mails alerts for the following endpoints events*.

Option	Description
Malware is detected.	Malware detected.
Repeated malware is detected.	Same malware is detected on the same machine in the last 24 hours.
Multiple malware detected.	Different malware is detected on the same machine in the last 24 hours.
Malware outbreak detected.	Same malware is detected on different endpoints in the last 24 hours.
Zero-day malware detected by FortiSandbox.	Previously unknown computer virus or other malware for which specific anti-virus software signatures are not yet available.
C&C attack communication channel is detected.	Command and control attack communication channel is detected.
Critical vulnerability is detected.	Critical vulnerability detected,
Endpoint FortiClient Telemetry is manually disconnected by user.	FortiClient Telemetry endpoint is manually disconnected by user.
Endpoint signature database is out-of-date.	Out-of-date Endpoint signature is detected.
Endpoint software is out-of-date.	Out-of-date Endpoint software is detected.

Automatic Updates

Following is a description of the field on the *View* > *Settings* > *Advanced* > *Automatic Updates*.

Option	Description
Automatic Updates	Enable to automatically download the latest updates and notify you to install.

User Management

This section describes the default user accounts and permissions for FortiClient EMS. It also describes how to change the administrator password and how to configure Windows users.

Default user accounts and permissions

The administrator has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment.

The administrator has access to all configured Windows and LDAP servers and users; and has the authority to configure user privileges and permissions.If you are not authorized for certain tasks or devices, the related menu items, items in content pages, and buttons are hidden or disabled. In addition, a message informs you that you do not have permission to view the selected information or perform the selected operation.

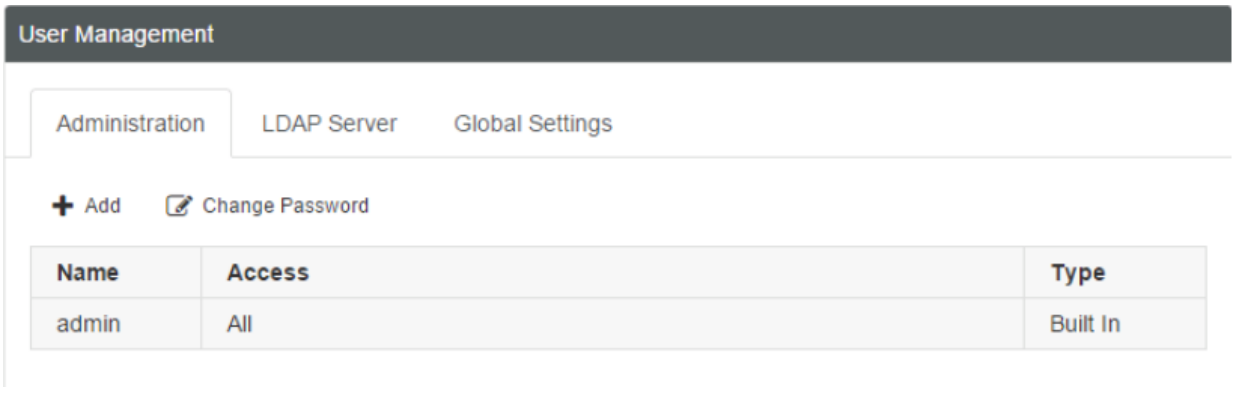
Configuring user management

Changing the Administrator Password

By default, the password is blank for the administrator account. You should add a password to increase security.

To change the administrator password:

1. Go to *View* > *User Management*.
2. Select the *Admin* account.
3. Click *Change Password* from the toolbar. Change your password.
4. Click *Save*.



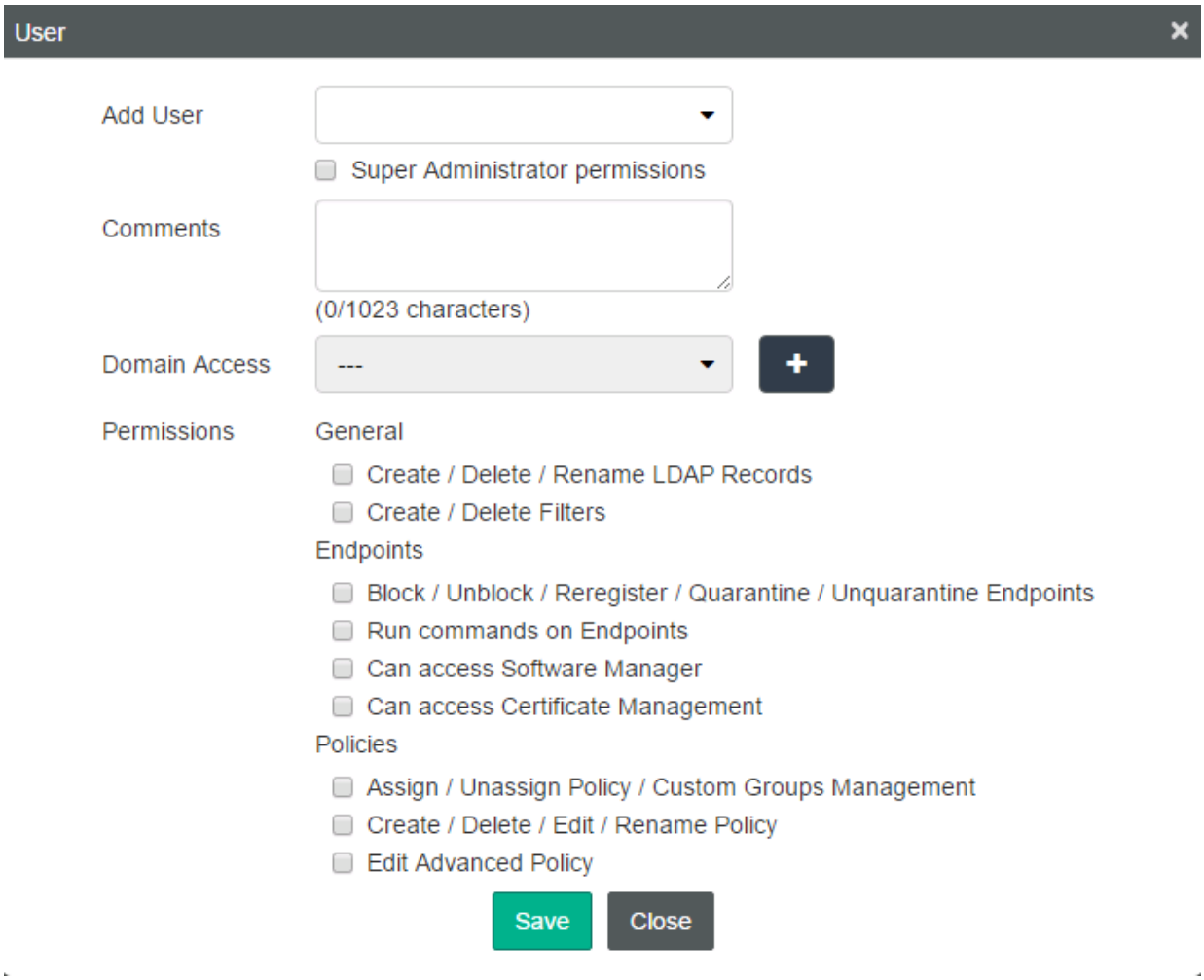
Configuring Windows User Accounts

You can configure Windows users to have no access to FortiClient EMS, or you can configure Windows users to have administrator access to FortiClient EMS.

The list of Windows users is derived from the server on which FortiClient EMS is installed. If you want to add more Windows users, you must add them to the server.

To configure Windows users:

1. Go to *View* > *User Management*.
2. Click the *+Add* button from the toolbar.
3. Expand the *Add User* drop-down menu.
4. Select the Windows User.
5. Perform one of the following actions:
   a. Select the specific domain access for the user. For a description of the permissions, see Default user accounts and permissions on page 38.
   b. Configure the permissions. For a description of the options, see Windows/LDAP Users on page 42.
6. Click *Save*.

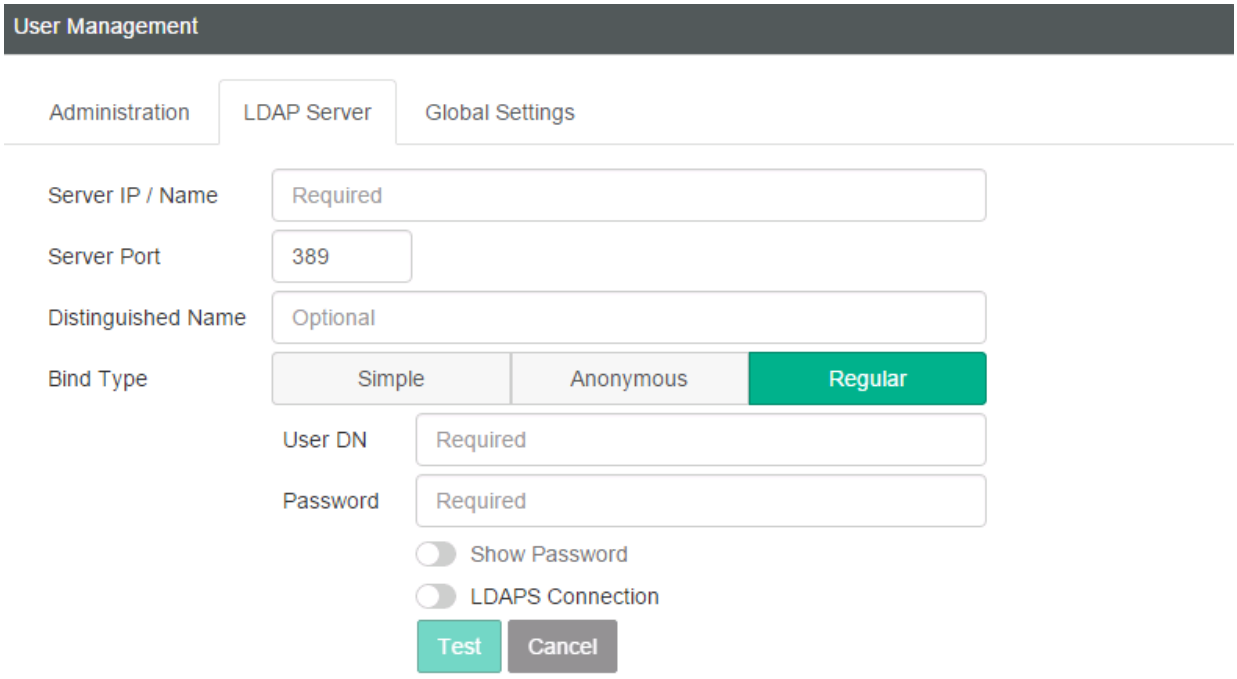


Configuring LDAP User Accounts

The list of LDAP users is derived from the server on which FortiClient EMS is installed. If you want to add more LDAP users, you must add them to the server.

To Add a new LDAP Server:

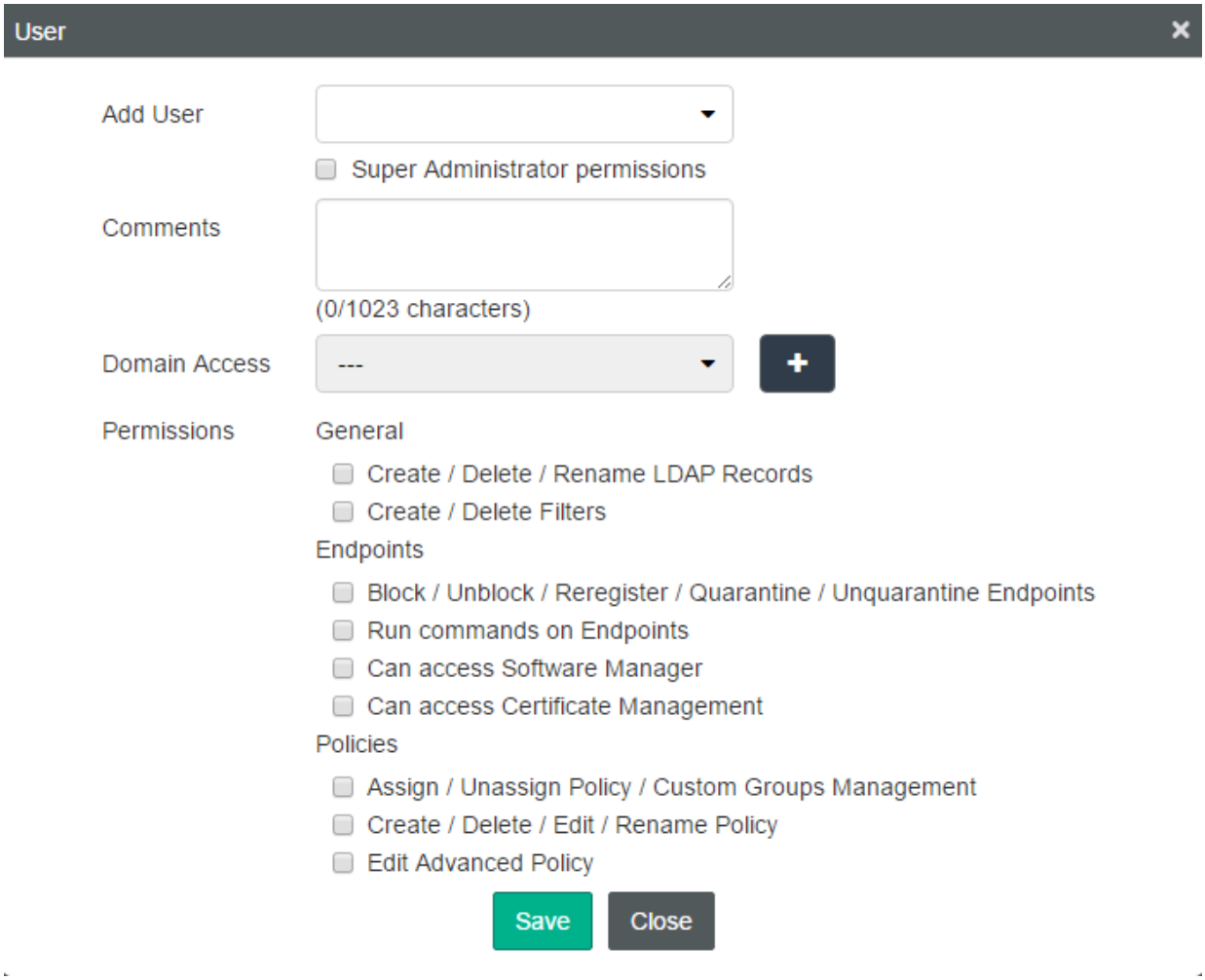
1. Go *View* > *User Management*.
2. Select the *LDAP Server* tab.
3. Configure the options. For a description of the options, see the User Management references on page 41.
4. Click *Save*.



To configure LDAP users:

1. Go to *View* > *User Management*.
2. Click the *+Add* from the toolbar.
3. Expand the *Add User* drop-down menu.
4. Select the LDAP User.
5. Perform one of the following actions.
6. Configure the options.
    a. Select the specific domain access for the user. For a description of the permissions, see Default user accounts and permissions on page 38.
    b. Configure the permissions. For a description of the options, see Windows/LDAP Users on page 42.

7. Click *Ok*.



User Management references

This section contains descriptions of the fields used to configure user management.

Administration

Following is a description of the fields on the *View* > *User Management* > *Administration* tab.

Option	Description
+Add	Add a new user.
Name	Name of the user.
Access	Type of user access.
Type	Type of user.

Windows/LDAP Users

Following is a description of the fields on the *View* > *User Management* > *Add* > *Windows/LDAP Users* .

Option	Description
User	Select the Windows/LDAP user for whom you want to configure permissions for FortiClient EMS.
Super Administrator Permissions	Enable the Super Administrator feature to give the new Windows/LDAP Users Super Administrator permissions.
Comments	Enter optional comments/information for the Windows/LDAP User.
Domain Access	Select or add a Domain Access for the Windows or LDAP User. If you select this option, you do not need to select specific permissions.
Permissions	Available only when *Administrator* is selected. Use the settings to configure permissions to FortiClient EMS for the selected Windows/LDAP User.
Create / Delete / Rename LDAP Records	Select to allow the Windows user to create, delete, and rename LDAP records. Clear to disable this permission.
Create / Delete Filters	Select to allow the Windows user to create and delete filters. Clear to disable this permission.
Endpoints	Use the following options to configure permissions for the selected Windows user.
Block / Unblock / Deregister / Quarantine / Unquarantine Endpoints	Select to allow the Windows user to block, unblock, deregister, quarantine, and unquarantine endpoints. Clear to disable this permission.
Run commands on Endpoints	Select to allow the Windows user to run commands on endpoints. Clear to disable this permission.
Can access Software Manager	Select to allow the Windows user to access the *View* > *Software Management* options. Clear to disable this permission.
Can access Certificate Management	Select to allow the Windows user to access the *View* > *CA certificate Management* options. Clear to disable this permission.
Assign / Unassign Policy / Custom Groups Management	Select to allow the Windows user to assign to endpoints and unassign profiles from endpoints as well as manage custom groups. Clear to disable this permission.
Create / Delete / Edit / Rename Policy	Select to allow the Windows user to create, delete, edit, and rename profiles. Clear to disable this permission.

Option	Description
Edit Advanced Policy	Select to allow the Windows user to use the advanced settings when editing a profile. Clear to disable this permission.

LDAP Server Tab

Option		Description
Server IP/Name		Enter the Server IP/Name.
Server Port		Enter the Server Port.
Distinguished Name		Enter a Distinguished Name.
Bind Type		Select either *Simple*, *Anonymous* or *Regular* for the Bind Type.
	User DN	Appears only when *Regular* bind type is selected. Enter the User DN.
	Password	Appears only when *Regular* bind type is selected. Enter the Password.
	Show Password	Enable Show Password.
	LDAPS Connection	Enable LDAPS Connection.
Test		Click to test the LDAP server settings.

Global Settings

Following is a description of the fields on the *View* > *User Management* > *Global Settings* tab.

Option	Description
Inactivity Timeout	Specify how long to keep inactive users logged into FortiClient EMS. When the time expires, the user is automatically logged out of FortiClient EMS. Type 0 to keep inactive users logged into FortiClient EMS indefinitely.

Endpoints

FortiClient Enterprise Management System (FortiClientEMS) needs to determine which devices it has to manage. Device information can come from either an Active Directory Service, Windows workgroup or manual FortiClient registration.

Adding Endpoints

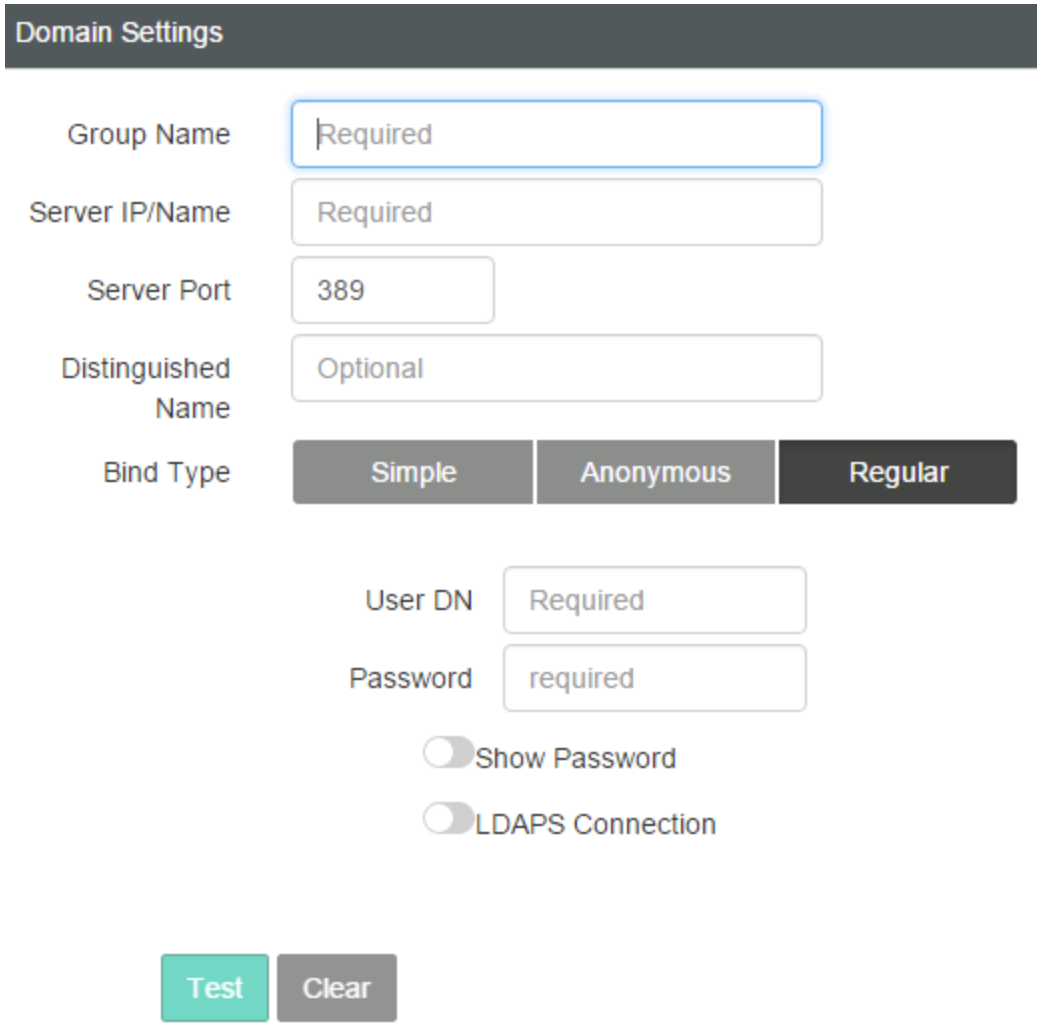
Adding Endpoints through an Active Directory Domain service

Endpoints can be manually imported from an Active Directory (AD) Domain Service. Users can import and synchronize information about computer accounts with a LDAP or STARTTLS service. You can add endpoints by identifying the endpoint devices that are part of an Active Directory (AD) domain service.

To search for endpoints using Active Directory Domain Service:

1. Click *Endpoints* > *Add a New Domain*.
2. In the *Domain Settings* page, set the options. For a description of the options, see Domain Settings pane on page

49.



3. Click *Test* to test the domain settings connection.
4. If the test is successful, select *Save* to save the new domain. If not, correct the information as required then test the settings again.

You cannot add, delete, or move groups within a domain.

Enabling an automatic discovery of endpoints with Windows workgroups

You can enable an automatic discovery of endpoint devices in local Windows workgroups.

To enable automatic discovery of workgroups:

1. Go to *View* > *Settings*.
2. Turn on *Scan local workgroups*. For a description of the options, see Server Settings Tab on page 33.
3. Click *Save*.
4. View the discovered endpoints in the *Endpoints* > *Workgroups* list.

Workgroups are listed under *Endpoints* > *Other Groups* . You cannot add, delete or move groups within a workgroup.

Registering manually from FortiClient

You can manually register FortiClient endpoints to FortiClient EMS by specifying the IP address for FortiClient EMS in FortiClient.

FortiClient 5.2.4 or later must be installed on the endpoint device to use the antivirus scan feature of FortiClient EMS.

To register an endpoint to FortiClient EMS

1. Ensure that FortiClient 5.2.4 or later is installed on the endpoint (device).
2. In FortiClient, select *Register to FortiGate*.
3. Enter the IP address configured for the FortiClient EMS. See FortiClient EMS Settings on page 30.
4. Select *Go* to register FortiClient.

For more information about endpoint management, refer to the *FortiClient Administration Guide* available on the docs.fortinet.com site.

The FortiClient Telemetry Gateway port may be appended to the FortiClient Telemetry Gateway IP List address on FortiClient and separated by a colon. When the port is not provided, FortiClient attempts to register to the IP address given by using the default port. The default registration port in FortiClient 5.2 is 8010 and in FortiClient 5.4 is 8013. FortiClient EMS listens for registration on port 8013 by default.

Viewing Endpoints

After FortiClient EMS has been populated by endpoints, users can view the details about its clients.

To view endpoints:

1. Go to *Endpoints* to view all endpoints.
2. Select an endpoint to view its details.

To view workgroups:

1. Go to *Endpoints* > *Workgroups* > *All Groups* to view all endpoints in the workgroups.
2. Select an endpoint to view its details.

To view domains:

1. Go to *Endpoints* > *select a Domain tree* to view all endpoints in the domain.
2. Select an endpoint to view its details.

To view manually registered FortiClient endpoints

1. Go to *Endpoints* > *Workgroups* > *All Groups* > *Other Endpoints* to view all endpoints that were manually registered.
2. Select an endpoint to view its details.

Managing endpoints

You can manage endpoints from the *Endpoints* pane. Some options are available as buttons, and some options are available in the right-click menu. Right-click an endpoint to display the menu.

Option	Description
Refresh	Refresh the list of domains or workgroups.
Show empty containers	Click to display a list of domains without endpoints.
Add a New Domain	Click to add a new Active Directory (AD) server to FortiClient EMS.
Assign profile	Select and apply a profile to the selected workgroup.
Unassign profile	Select to unassign a profile from a selected workgroup.
Assign FortiClient Telemetry Gateway IP List	Right-click to assign a FortiClient Telemetry Gateway IP List.
Unassign FortiClient Telemetry Gateway IP List	Select to unassign a FortiClient Telemetry Gateway IP List.
Exclude from management	Select to exclude the selected workgroup from management by FortiClient EMS. You can also exclude individual endpoints within the workgroup from management by FortiClient EMS.
Enable management	Select to enable FortiClient EMS to manage the selected workgroup. You can also enable management by FortiClient EMS for individual endpoints within the workgroup.
Create group	Select to create a group or subgroup. You can then move devices into the group or subgroup.
Rename group	Select to rename the selected group or subgroup.
Delete group	Select to delete the selected group or subgroup.
Move devices	Select to move the devices from the selected group to another group.
Full AV scan	Select to start a full antivirus scan on the selected workgroup.

Option	Description
Quick AV scan	Select to start a quick antivirus scan on the selected workgroup.
Vulnerability Scan	Select to start a Vulnerability Scan on the selected endpoint.
Patch Critical and High Vulnerabilities	Select to patch critical and high vulnerabilities on the selected endpoint.

Updating FortiClient endpoints

You can update FortiClient on endpoints by editing the profile associated with the endpoint. When you save the profile, the changes are automatically pushed to the FortiClient endpoints.

If you enable the Auto-Sync FortiClient Profiles with FortiGate, users can can auto-sync profile changes to FortiClient EMS once its been modified on the FortiGate. For more information, see Configuring profiles on page 55.

Endpoint status

Viewing endpoint status

You can monitor endpoint status within FortiClient EMS. Use the right content pane to review the following endpoint information:

- Endpoint status
- System information
- FortiClient registration information
- Outdated versions of FortiClient on the endpoint computers

To view endpoint status:

1. Go to *Endpoints*. A list of all endpoints and information about each endpoint is displayed.
2. Select an endpoint to view more details.

Endpoint references

This section contains descriptions of the fields used to discover endpoints.

Domain Settings pane

Following is a description of the fields on the *Endpoints* > *Domains* > *Add a domain* pane.

Option	Description
Group Name	Enter a name for the group. The name will be displayed in the FortiClient EMS Endpoint view
Server IP/ Name	Type the IP address or name.
Server Port	Type the port number.
Distinguished Name	Type the distinguished name (optional).
Bind Type	Select the bind type. Simple, Anonymous, Regular . When you select *Regular*, enter the User DN and password.
User DN	Available when *Bind Type* is set to *Regular*. Type the user DN.
Password	Available when *Bind Type* is set to *Regular*. Type the user password.

Option	Description
Show Password	Available when *Bind Type* is set to *Regular*. Turn on and off to show or hide the password.
Secure Connection	Turn on to enable a secure connection protocol.
Test	Tests the domain settings connection. If the test is successful, select *Save* to save the new domain. If not, correct the information as required, and then test the settings again.
Clear	Reset the content of the *Domain Settings* page.

Installers

FortiGuard Distribution Network

FortiClient EMS automatically connects to FortiGuard Distribution Network (FDN) to provide access to FortiClient installers that you can use with FortiClient EMS profiles. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS.

Adding installers

Adding FortiClient installers to FortiClient EMS

When a connection to FortiGuard Distribution Network (FDN) is available, FortiClient installers are available in FortiClient EMS for you to select in FortiClient EMS. You must select and add the FortiClient installers that you want to use to FortiClient EMS, so you can use the installers with profiles.

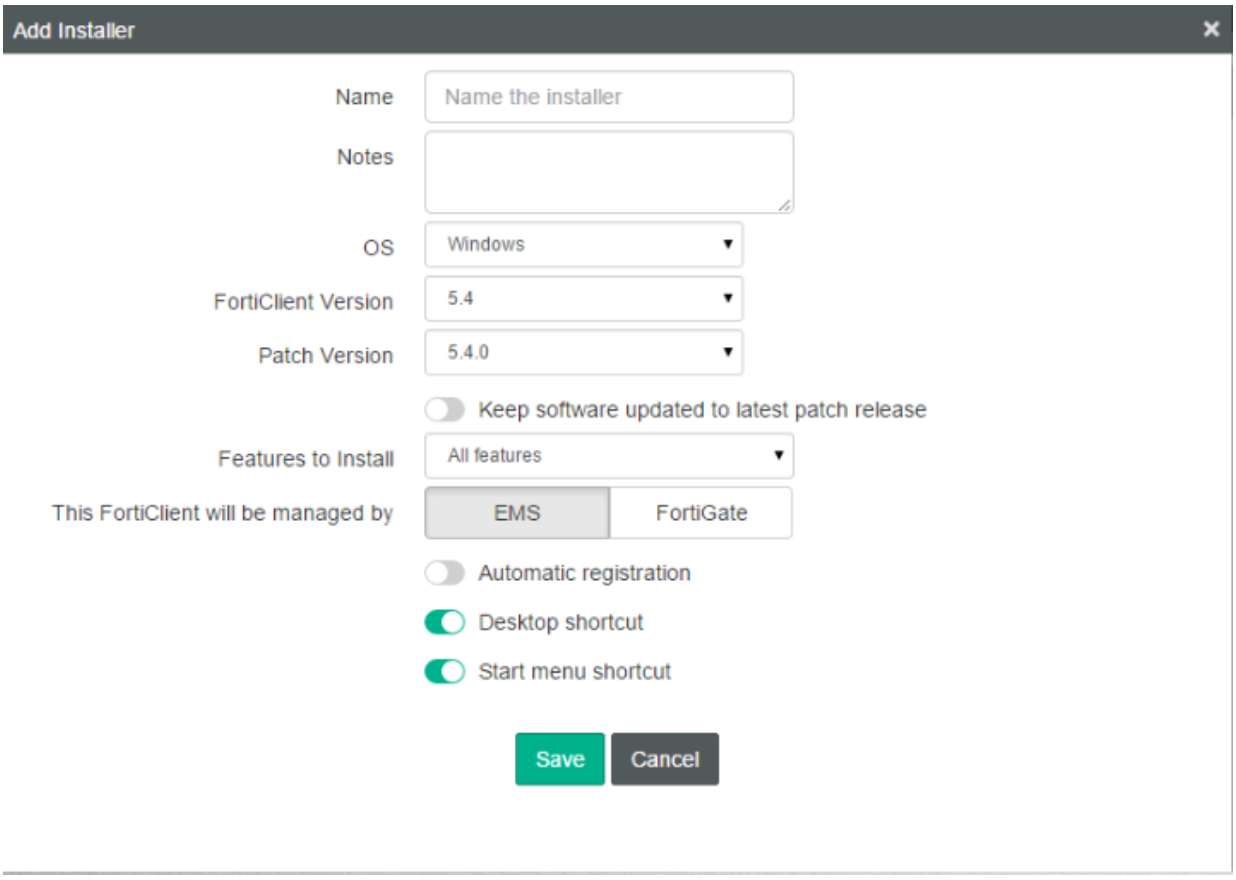
When you add the installer to FortiClient EMS, you can specify what FortiClient features to include in the installer for the endpoint. You can include a feature in the installer, and then disable the feature in the profile. Because the feature is included in the installer, you can update the profile later to enable the feature on the endpoint.

You can also specify whether FortiClient EMS or FortiGate will manage the endpoint after FortiClient is installed.

You cannot edit a FortiClient installer after you add it to FortiClient EMS. You can delete the installer, and add it again.

To add FortiClient installers to FortiClient EMS:

1. Go to *View* > *Software Manager*. The *FortiClient Software Manager* pane is displayed.
2. Click the *+ Add* button.



3. Select a FortiClient installer, and configure the options. For a description of the options, see Add Installer reference on page 53.
4. Click *Save*. The installer is added to FortiClient EMS and displayed on the *FortiClient Software Manager* pane.

Adding custom FortiClient installers to FortiClient EMS

You can create a custom FortiClient installer and add it to FortiClient EMS. Alternately, if a connection to FDN is not available, you might need to manually download a FortiClient installer and add it to FortiClient EMS. For more information, see FortiGuard Distribution Network on page 51.

To add custom FortiClient installers to FortiClient EMS:

1. Download a FortiClient installer.
2. Go to *View* > *Software Manager*. The *FortiClient Software Manager* pane is displayed.
3. Click *Add*. The Add Installer pane is displayed.
4. In the *FortiClient Version* list, select *Upload*. For a description of the options, see Add Installer reference on page 53.
5. Click the *Browse* button, and select the custom installer.
6. Click *Save*. The installer is added to FortiClient EMS and displayed on the *FortiClient Software Manager* pane.

Installer references

This section contains descriptions of the fields used to configure installer packages.

Add Installer reference

Following is a description of the fields on the Add Installer page.

Option	Description
Name	Type a descriptive name for the installer.
Notes	(Optional) Type notes about the installer.
OS	Select *Mac OS X* or *Windows* to identify the operating system for which the installer file is created.
FortiClient Version	Select the installer for the FortiClient version that you want to deploy to endpoints.
Patch Version	Select the patch version for the FortiClient installer if applicable.
Keep software updated to latest patch release	Enable to keep FortiClient EMS up to date with the latest patch release.
Features to install	Available when *OS* is set to *Windows*. Select what features you want to include in the FortiClient installer. Only selected features are included in the installer. Excluded features are excluded from the installer. You can configure selected features when you configure the FortiClient EMS profile.
This FortiClient will be managed by	Available when *OS* is set to *Windows*. Select *EMS* or *FortiGate* to identify whether FortiClient EMS or FortiGate will manage the endpoints after FortiClient is installed. You must also select the IP address for the FortiClient EMS or FortiGate that will manage the endpoint. The FortiClient endpoint uses the IP address to automatically register with the management server. For example, if FortiClient EMS will manage the FortiClient endpoint, select the IP address for FortiClient EMS. If FortiGate will manage the FortiClient endpoint, select the IP address for the FortiGate.
Automatic registration	Available when *OS* is set to *Windows*. Turn on for FortiClient endpoints to automatically register with the management server, which is either FortiClient EMS or FortiGate. Turn off to disable automatic registration with management server.
Desktop shortcut	Available when *OS* is set to *Windows*. Turn on for a FortiClient desktop shortcut to be created when FortiClient is installed on endpoints. Turn off to disable this feature.

Option	Description
Start menu shortcut.	Available when *OS* is set to *Windows*. Turn on for a FortiClient start menu shortcut to be created when FortiClient is installed on endpoints. Turn off to disable this feature.
FortiClient Installer	Available when *OS* is set to *Mac OS X*. Select the FortiClient installer that you created for Mac OS X.
FortiClient Installer (64 bit)	Select the 64-bit FortiClient installer that you created.
FortiClient Installer (32 bit)	Select the 32-bit FortiClient installer that you created.

Profiles

XML configuration

You can configure FortiClient profile settings in FortiClient EMS by using a custom XML configuration file. The custom file includes all settings required by the endpoint at the time of deployment. When the endpoint registers to FortiClient EMS, ensure the complete XML configuration file is used. For more information about how to configure a profile with XML, see the *FortiClient XML Reference* on docs.fortinet.com

Configuring profiles

Importing FortiGate profiles

You can import profiles from FortiGate to FortiClient EMS and use the profiles with FortiClient EMS.

Due to compliance rules set in the FortiGate, the FortiClient EMS administrator cannot change the features or options configured on the FortiGate. However, administrators can configure features or options that are FortiClient EMS specific; for example, adding a VPN configuration.

To import profiles:

1. Click *Endpoint Profiles* > *Import Profile from FortiGate*.
2. Complete the options, and click *Next* until you complete the wizard.

To import FortiGate profiles successfully to FortiClient EMS, FortiGate must have the HTTPS port open. Go to *Network* > *Interfaces* > *Restrict Access* > *Enable checkbox for HTTPS*.

Auto-Sync FortiClient Profiles with FortiGate

Manage profile configurations from one place while using FortiClient EMS to manage client deployment. Once profiles have been modified on the FortiGate, users can auto-sync the profile changes to FortiClient EMS.

To Auto-Sync FortiClient Profiles with FortiGate

1. Select a profile imported from FortiGate.
2. Go to the *Auto-Sync Settings* tab.
3. Enable the *Endpoint Profile Auto-Sync Settings*.
4. Configure the options. For a description of the options, see Profile references on page 57.

Adding new profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any groups that you create. The default profile is designed to provide effective levels of protection. If you want to use specific features, such as application firewall, you can create a new profile or change the default profile.

Consider the following when creating profiles:

- Use default settings within a profile.
- Consider the role of the computer when changing default profile or creating new profiles.
- Create a separate group and profile for computers that require long-term special configuration.
- Use FortiClient EMS for all central profile settings, and set options for within the group instead of for the computer itself when possible.

To add new profiles:

1. Go to *Endpoint Profiles* > *Add a new profile*.
2. On the *Install Options* tab, select a FortiClient installer from the *FortiClient Deployment* list.

   The selected installer controls what tabs are displayed for the profile, based on the features that the installer includes. For example, if the installer includes only the VPN feature, only the *VPN* tab is displayed for you to configure. The *System Settings* tab is always displayed.

   You can disable a feature that is included in the installer, and then enable the feature in the profile at a later date. For example, if the installer includes the Web Filter and VPN features, you can disable the Web Filter feature and keep the VPN feature enabled. When FortiClient is installed on the endpoint, the Web Feature is installed, but disabled.
3. Configure the settings on the tabs. For a description of the options, see Profile references on page 57.
4. Click *Save* to save the profile.

You have the option to schedule an installation. Go to *Profile* > *Install Options* > *FortiClient Installer Settings* > *Schedule Installation*.

Vulnerability Scan Settings

1. Select an *Endpoint Profile*.
2. Go to the *Vulnerability Scan Settings* tab.
3. Configure the options. For a description of the options, see Profile references on page 57.

Pushing profile changes to endpoints

Assigning profiles to endpoints

After creating the profile, you can assign the profile to domains or workgroups. When you assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

To assign profiles:

1. Go to *Endpoints*
2. Right-click a domain or group, select *Assign Profile*, and then the profile. The profile is assigned.
3. Hover the mouse over the name of the domain or group to view the name of the assigned profile.

Editing profiles

When you edit a profile that is assigned to endpoints, the changes are automatically pushed to the endpoints when you save the profile.

To update profiles:

1. Go to *Endpoint Profiles* > *EMS Profiles*, and select a profile. The profile settings are displayed in the content pane.
2. Edit the settings. For a description of the options on the tabs, see Profile references on page 57.
3. Click *Save*. The changes are installed on the endpoints associated with the profile.

Managing profiles

You can manage profiles from the *Endpoint Profiles* pane by clicking the icons.

Option	Description
Refresh	Refresh the list of profiles.
Import	Click to import a profile from FortiGate.
Add a New Profile	Click to create a new profile.
Revert to default	Click to revert the default profile to its default settings.
Edit	Select a profile to display its settings in the content pane for editing.
Clone	Click to clone the profile.
Delete	Click to delete the profile.

Profile references

This section contains descriptions of the fields used to configure profiles.

Endpoint Profile pane

Configuration	Description
Profile Name	Type a name for the profile.
Basic	Select to configure the profile by using the GUI.
Advanced	Select to configure the profile by using XML.

Basic Settings

Install Options

Option	Description
Name	Type a descriptive name for the installer.
Notes	(Optional) Type notes about the installer.
OS	Select *Mac OS X* or *Windows* to identify the operating system for which the installer file is created.
FortiClient Version	Select the installer for the FortiClient version that you want to deploy to endpoints.
Patch Version	Select the patch version for the FortiClient installer if applicable.
Keep software updated to latest patch release	Enable to keep FortiClient EMS up to date with the latest patch release.
Features to install	Available when *OS* is set to *Windows*. Select what features you want to include in the FortiClient installer. Only selected features are included in the installer. Excluded features are excluded from the installer. You can configure selected features when you configure the FortiClient EMS profile.
This FortiClient will be managed by	Available when *OS* is set to *Windows*. Select *EMS* or *FortiGate* to identify whether FortiClient EMS or FortiGate will manage the endpoints after FortiClient is installed. You must also select the IP address for the FortiClient EMS or FortiGate that will manage the endpoint. The FortiClient endpoint uses the IP address to automatically register with the management server. For example, if FortiClient EMS will manage the FortiClient endpoint, select the IP address for FortiClient EMS. If FortiGate will manage the FortiClient endpoint, select the IP address for the FortiGate.

Option	Description
Automatic registration	Available when *OS* is set to *Windows*. Turn on for FortiClient endpoints to automatically register with the management server, which is either FortiClient EMS or FortiGate. Turn off to disable automatic registration with management server.
Desktop shortcut	Available when *OS* is set to *Windows*. Turn on for a FortiClient desktop shortcut to be created when FortiClient is installed on endpoints. Turn off to disable this feature.
Start menu shortcut.	Available when *OS* is set to *Windows*. Turn on for a FortiClient start menu shortcut to be created when FortiClient is installed on endpoints. Turn off to disable this feature.
FortiClient Installer	Available when *OS* is set to *Mac OS X*. Select the FortiClient installer that you created for Mac OS X.
FortiClient Installer (64 bit)	Select the 64-bit FortiClient installer that you created.
FortiClient Installer (32 bit)	Select the 32-bit FortiClient installer that you created.
Uninstall FortiClient	
Use these credentials to uninstall	Enter *username* and *password* to uninstall FortiClient.

AntiVirus Protection

Options	Description
Antivirus Protection	Enable antivirus protection. Configure the following options:

Options		Description
	Real Time Protection	Enable real-time protection. • Scan files as they are downloaded or copied to my system. • Extended scanning using FortiSandbox. An IP address is required. a. Deny Access to file until FortiSandbox results are received. b. Deny access to downloaded files if FortiSandbox is offline c. Identify malware & exploits using signatures received from FortiSandbox. • Block known communication channels used by attackers • Block all access to malicious websites. a. You have the option to use the exclusion list defined in the Web Filter Profile. • Alert when viruses are detected
	Scheduled Scan	Enable scheduled scans, and then enter the following: • Schedule Type: Daily, Weekly, or Monthly. • Scan On: If Weekly is selected, select the day of the week to perform the scan. If Monthly is selected, select the day of the month to perform the scan. • Start: Select the start time for the scheduled scan. • Scan Type: Quick system scan, Full system scan, or Custom scan. If Custom scan is selected, enter the full path of the folder that will be scanned in the Folder field.
	Exclusions	Enable exclusions from the scan. Enter fully qualified excluded folder paths or files in the provided text box to exclude these folders and add files from antivirus scanning.
Show Advanced Options		Turn on to display and configure basic and advanced options. Turn off to display and configure only basic options.

Options		Description
	Real Time Protection	Enable real-time protection. • Scan files as they are downloaded or copied to my system. a. Clean infected files (quarantine if cannot clean) b. Repair infected files (quarantine if cannot clean) c. Warn the user if a process attempts to access infected files d. Quarantine infected files e. Deny access to infected files • Extended scanning using FortiSandbox. An IP address is required. a. Deny Access to file until FortiSandbox results are received. b. Deny access to downloaded files if FortiSandbox is offline c. Identify malware & exploits using signatures received from FortiSandbox. • Block known communication channels used by attackers • Block all access to malicious websites. a. You have the option to use the exclusion list defined in the Web Filter Profile. • Alert when viruses are detected

Options	Description	
	One Demand	a. Clean infected files (quarantine if cannot clean) b. Quarantine infected file (quarantine if cannot clean) c. Warn the user if a process attempts to access infected files d. Quarantine infected files • Integrate FortiClient into Windows Explorer's mouse menu • Pause scanning when running on battery pwer • Automatically submit suspicious files to FortiGuard for analysis • Scan compressed files. a. Configure the max file size. b. Configure the max scan speed on computer with more than 4GB-16GB of memory installed.
	Scheduled Scan	• Scan removable media, if present • Scan network drives • Enabled scheduled scans even when a third party AV product is present
	Exclusions	• File extensions excluded from Real Time AntiVirus Protection • File Extensions excluded from On Demand AntiVirus Protection
	More Options	• Scan for rootkits • Scan for adware • Scan for riskware • Enable advanced heuristics • Scan removable media on insertion • Scan mime files (inbox files) • Enable FortiGuard Analytics • Notify logged in users if their AntiVirus signatures expire

Web Filter

Configuration	Description
Web Filter	Enable web filtering. • Client Web Filtering when On-Net • Enable FortiGuard URL categorization: Block, Warn, Allow, or Monitor specific categories of web sites. See the FortiGuard web site for descriptions of the available categories and subcategories. • Rate IP addresses: Select to rate IP addresses. • Exclusion List: Enter specific URLs to block or allow. Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used.
Show Advanced Options	Turn on to display and configure basic and advanced options. Turn off to display and configure only basic options.
Web Filter	• Log All URLs • Log user initiated traffic

Application Firewall

Configuration	Description
Application Firewall	Enable application control.
Notification bubbles on user's desktop when applications are blocked	Enable notification bubbles when applications are blocked.
Detect & Block Exploits	Enable to detect and block exploits.

Configuration		Description
Categories		Block, allow or monitor the following categories: **a.** IM **b.** P2P **c.** VoIP **d.** Video/Audio **e.** Proxy **f.** Remote Access **g.** Game **h.** General Interest **i.** Network Service **j.** Update **k.** Botnet **l.** Email **m.** Storage Backup **n.** Social Media **o.** File Sharing **p.** Web Other **q.** Industrial **r.** Special **s.** Collaboration **t.** Business **u.** Cloud IT **v.** Mobile **w.** All other known applications **x.** All other unknown applications
Application Overrides		
	Delete	Delete an application.
	Add Signature	Add a signature to an application.

VPN

Configuration	Description
VPN	Enable VPN use.
Allow Personal VPN	Enable to allow personal VPN.
Disable Con-nect/Disconnect	Enable to disable connect/disconnect.

Configuration		Description
Show VPN Before Logon		Enable to show VPN before logon.
Local Computer Windows Store Certificates (IPSec only)		Enable local computer Windows Store certificates (IPSec only).
Current User Windows Store Certificates (IPSec only)		Enable current user Windows Store certificates (IPSec only).
SSL VPN		Enable SSL VPN.
IPSec VPN		Enable IPSec VPN.
Add VPN Tunnel		
	VPN Name	Enter a VPN name.
	Type	Select either SSL VPN or IPSec VPN for the type.
	Remote Gateway	Enter an IP address or hostname.
	Require Certificate	Enable to require a certificate.
	Access Port	Enter the access port.
Show advanced options		Enable to display and configure advanced options. .
Minimize Window on Connect		Enable to minimize the window upon connecting.
Show Negotiation Window		Enable to show negotiation window.
Current Connection		
Auto-connect		
	Auto-connect only when Off-Net	Enable to automatically connect when Off-net.
	Keep Running Maximum Tries	Configure the maximum number of tries.
SSL VPN		

Configuration		Description
	DNS Cache Service Control	Enable for DNS Cache Service Control. When this setting is 0, the custom DNS server from SSL VPN will not be added to physical interface. When this setting is 1, custom DNS server from SSL VPN will be prepended to physical interface.
	Prefer SSL VPN DNS	Enable to prefer SSL VPN DNS.
IPSec VPN		Enable or disable the following: **a.** Beep if Error **b.** Local Computer Windows Store Certificates (IPSec only) **c.** Current User Windows Store Certificates (IPsec only) **d.** Use Windows Store Certificates **e.** Use Local Certificates **f.** Use Smart Card Certificates **g.** Show Auth Certificates Only **h.** Block IPv6 **i.** Enable UDP Checksum **j.** Disable Default Route **k.** Check For Certificate Private Key **l.** Enhanced Key Usage Mandatory **m.** Use Vendor ID
Add VPN Tunnel		
	Single User Mode	Enable Single User Mode.
	Warn on Invalid Server Certificate	Enable to warn when an invalid server certificate is used.
	Remember Password option	Enable to remember password.
	Always Up option	Enable to have the VPN Tunnel always up.
	Auto Connect option	Enable to auto connect the VPN Tunnel.
	On Connect Script	Enable the On Connect script.
	On Disconnect Script	Enable the Disconnect script.

Vulnerability Scan

Configuration	Description
Vulnerability Scan Settings	Enable Vulnerability Scan Settings.
Scan on registration	Scan endpoints upon registering to a FortiGate.
Scan on signature update	Scan endpoints upon updating a signature.
Schedule Scan	Schedule the scan.
Schedule Type	Configure either *Daily*, *Weekly*, *Monthly*.
Scan On	Configure the day the scan will run (1st-31st of the month). This only applies if the Schedule Type is configured to *Monthly*.
Start	Configure the time the scan will start.
Scan and Patch Windows Updates	Scan and patch when there are Windows updates
Automatically Patch Vulnerabilities	When enabled, patches will be installed automatically when vulnerabilities are detected. **a.** Patch critical vulnerabilities only **b.** Patch high severity, and above, vulnerabilities **c.** Patch medium severity, and above, vulnerabilities **d.** Patch low severity, and above, vulnerabilities **e.** Patch all vulnerabilities.

System Settings

Configuration	Description
UI options	Specify how the FortiClient user interface will appear when installed on endpoints.
Dashboard Banner	Turn on to display the dashboard banner in FortiClient. Turn off to hide the dashboard banner.
Password Lock Configuration	Turn on the password lock for FortiClient.
Password	Type a password in the Password field. Select Show Password to show the password in plain text.
Log Settings	Specify the log settings for FortiClient.

Configuration		Description
	Client-based Logging when On-Net	Turn on client-based logging when On Net. For more information about using the on-net feature, see the FortiClient Administration Guide.
	Upload Logs to FortiAnalyzer/FortiManager	Turn on to upload FortiClient logs to the FortiAnalyzer or FortiManager device at the specified address or hostname. You can enable the following: • Upload Traffic Logs • Upload Vulnerability Logs • Upload Event Logs Enter the following: • IP Address • Upload Schedule in minutes • Log Generation Time out in seconds.
Update Settings		Specify whether to use FortiManager to update FortiClient on endpoints
	Use FortiManager for clientsoftware/signature update	Turn on to enable FortiClient EMS to obtain antivirus signatures and software updates from the FortiManager device at the specified IP address or hostname. If required, enable Failover to FDN when FortiManager is not available. Enter the following: • IP Address/hostname • Port You can enable the following: • Failover to FDN when FortiManager is not available.
Endpoint Control Settings		Specify settings for the endpoints.
	Silent Registration	Turn on to enable silent registration of endpoints, which means that endpoints are registered without user interaction. Turn off to require user interaction to register endpoints.
	Log off when user logs out of Windows	Turn on to log off FortiClient when the endpoint user logs out of Windows. Turn off to remain logged in.
	Disable Unregister	Turn on to forbid users from unregistering FortiClient from FortiClient EMS. Turn off to allow users to unregister FortiClient from FortiClient EMS. You can enable the following: • Disable FGT Switch

Configuration		Description
	Onnet Subnets	Turn on to enable onnet subnets. Enter the following: • IP Addresses/Masks You can enable the following: • Gateway Mac Addresses
Other Options		
	Install CA Certificate on Client	Turn on to select and install a CA certificate on the FortiClient endpoint. You can add certificates by going to *View* > *CA Certificate Management*.
	FortiClient Single sign-On mobility agent	Turn on to enable the single sign-on mobility agent. Enter the following: • IP address or hostname • Port • Pre-shared key. You can enable the following: • Show Password
iOS		
	Distribute Configuration Profile (.mobileconfig file)	Turn on to select and distribute a configuration profile to FortiClient endpoints.
Show Advanced Options		Enable to display and configure advanced options. .
	UI Options	Hide System Tray Icon • Configure the Culture Code

Configuration	Description
Log Settings	Levels • Configure the level: a. Emergency b. Alert c. Critical d. Error e. Warning f. Notice g. Information h. Debug Features • You can enable the following: a. IPSec VPN b. SSL VPN c. Update d. Application Firewall e. AntiVirus f. Proxy g. Web Filter h. Endpoint Control i. FSSOMA j. Wan Optimization Upload Logs to FortiAnalyzer/FortiManager • Upload Event Logs. Configure the following: a. IP Address/Hostname • SSL Enabled. Configure the following: a. Upload Schedule in minutes b. Log Generation Timeout in seconds c. Log Retention in days
Proxy Settings	• Use proxy for updates. Configure the following: a. Type b. IP address/hostname c. Port d. User Name e. Password • Use proxy for virus submission

Configuration		Description
	Update Settings	Auto Patch • Configure the following: a. Update Action b. Notify Only c. Download and Install d. Download only • Update Schedule a. Configure either: Hourly or Daily b. Interval
	FortiProxy Settings	Only disable when troubleshooting • You can enable the following a. HTTP Proxy: Configure the timeout in seconds b. POP3 client comforting c. POP3 server comforting d. SMTP e. SelfTest f. Notify: Enter the port
	Other Options	Wan Optimization • Configure the following: a. Maximum Disk Cache Size: 512 or 1024 MB

Advanced Settings

Configuration Tab

Configuration	Description
XML Editor	Configure using the XML Editor.

Auto-Sync Settings Tab

Configuration	Description
Endpoint Profile Auto-Sync Settings	Enable Endpoint Profile Auto-Sync Settings.
Automatically check for profile updates from FortiGate and deploy to endpoints	Specify the time interval to check for updates.

FortiClient Telemetry Gateway IP Lists

FortiClient Telemetry Gateway IP Lists

About FortiClient Telemetry Gateway IP Lists

FortiClient Telemetry Gateway IP List feature allows greater control of FortiClient Telemetry client registration. Instead of managing and monitoring endpoints from FortiGate or FortiClient EMS, this feature de-couples the FortiGate IP List from the rest of the profile. This allows EMS administrators to dictate where the FortiClient Telemetry clients register to.

The user creates a list of IP addresses to register to. This becomes the FortiClient Telemetry Gateway IP List. To deploy, assign the FortiClient Telemetry Gateway IP List to a domain or workgroup. After deployment and FortiClient Telemtery data registration process has started, the endpoint will try to register to a FortiGate or EMS. This registration is based on the FortiClient Telemetry Gateway IP List received from EMS.

Even if the endpoint is already registered to a FortiGate, users can still assign a FortiClient Telemetry Gateway IP List. Users can also update list as required. The updates will then be pushed to the its clients.

Creating FortiClient Telemetry Gateway IP Lists

Create a FortiClient Telemetry Gateway IP List

1. Go to *FortiClient Telemetry Gateway IP List*
2. Click the **+** button.

3. Configure the following:

List Name	Enter the list name.
Comment	Enter additional comments (optional).
IP Addresses	Enter the IP address and port for FortiGate devices by using the following format: IP:port
Connection Key (Optional)	Enable the registration key for FortiGate devices that FortiClient endpoints can use for registration.
Connection Key	Enter the registration key.
Confirm Key	Re-enter the registration key to confirm.
EMS IP/FQDN	Enter the EMS IP/FQDN. Users can configure this IP address in the *View* > *Settings* page.

4. Click *Save*.

Assigning FortiClient Telemetry Gateway IP Lists to endpoints

Assigning FortiClient Telemetry Gateway IP Lists to endpoints

After creating the FortiClient Telemetry Gateway IP List, you can assign the list to endpoints. When you assign the IP list and FortiClient Telemetry data registration process has started, the endpoint will register to a FortiGate based on the FortiClient Telemetry Gateway IP List.

Assign a FortiClient Telemetry Gateway IP List

1. Select a domain or workgroup.
2. *Right-click* > *Assign FortiClient Telemetry Gateway IP List* > *Select List*.

Viewing Assigned FortiClient Telemetry Gateway IP Lists

View an Assigned Endpoint's FortiClient Telemetry Gateway IP List

1. Select an Endpoint.
2. *FortiClient Information* > *Gateway IP List* column.

Deployment and updates

You can use FortiClient EMS to deploy FortiClient on the endpoint devices that are part of an Active Directory (AD) server. Deploying FortiClient from FortiClient EMS requires the following steps:

- Preparing the AD server for deployment
- Deploying FortiClient on endpoint devices

After FortiClient is deployed on endpoints, and endpoints are registered with FortiClient EMS, you can update endpoints by editing the profiles associated with endpoints. Profile changes are automatically pushed to the endpoints.

Preparing the AD Server for Deployment

Before you can successfully deploy a FortiClient installation, ensure that you install and prepare the AD server as follows:

- Configure a group policy on the AD server.
- Configure the required Windows services on the AD server.
- Create deployment rules for Windows firewall
- Configure Windows firewall domain profile settings

Configuring a Group Policy on the AD Server

To configure a group policy on the AD server:

1. On the AD server, open *Group Policy Management*.
2. Right-click the *Default Domain Policy* setting. The Group Policy Management Editor opens.
   A new policy will be applied to the entire AD domain. Alternatively, you can create a new Group Policy Object, and link it to one or more organizational units (OU) in the AD server that contains the endpoint computes on which FortiClient will be deployed.

Configuring Required Windows Services

To configure required Windows services:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *System Services*.
2. In the right panel, select the following:
   a. Task Scheduler: Automatic
   b. Windows Installer: Manual
   c. Remote Registry: Automatic

Creating Deployment Rules for Windows Firewall

To create deployment rules for Windows firewall:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Windows Firewall with Advanced Security* > *Inbound Rules*.
2. Right-click *Inbound Rules* and select *New Rule*.
3. Select *Predefined* from the drop-down list and select *File and Printer Sharing*.
4. Click *Next*.
5. Ensure that the *File and Printer Sharing (SMB-In)* box is select and click *Next*.
6. Select *Allow the connection* and click *Finish*.
7. Repeat steps 1 to 2.
8. Select *Predefined* from the drop-down list and select *Remote Scheduled Tasks Management* and click *Next*.
9. Ensure that the *Remote Scheduled Tasks Management (RPC)* box is checked and click *Next*.
10. Select *Allow the connection* and click *Finish*.

Configuring Windows Firewall Domain Profile settings

To configure Windows firewall domain profile settings:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Administrative Templates* > *Network* > *Network Connections* > *Windows Firewall* > *Domain Profile*.
2. Select *Allow inbound file and printer sharing* exception:
   a. Right-click and select *Edit*.
   b. Enable the radio button.
   c. Provide the IP address of the EMS server in the text box.
   d. Allow unsolicited incoming messages from these IP addresses.
   e. Click OK.
3. Select *Allow inbound file and remote administration* exception:
   a. Repeat steps listed in step 2 above to create an exception.

To deploy the group policy manually, execute `gpupdate /force` on the AD server to update the group profile on all endpoint clients.

Execute `gpresult.exe /H gpresult.html` on any AD client to view the group policy deployed on the endpoints.

Deploying FortiClient on endpoint devices

Before you can successfully deploy a FortiClient installation from FortiClient EMS by using an AD server, you must have prepared the AD server. See Preparing the AD Server for Deployment on page 74.

To deploy FortiClient on endpoint devices

1. Add the AD server to FortiClient EMS by adding a domain. See Adding Endpoints on page 44.
2. Add a FortiClient installer package to FortiClient EMS. See Adding installers on page 51.
3. Add a profile, select the FortiClient installer package, and configure FortiClient features in the profile. See Configuring profiles on page 55.
4. Assign the profile to a branch of the AD domain to push the FortiClient installation process on the endpoint devices. See Assigning profiles to endpoints on page 56.
5. Verify the deployment by monitoring FortiClient registrations to the FortiClient EMS.

To deploy to workgroups

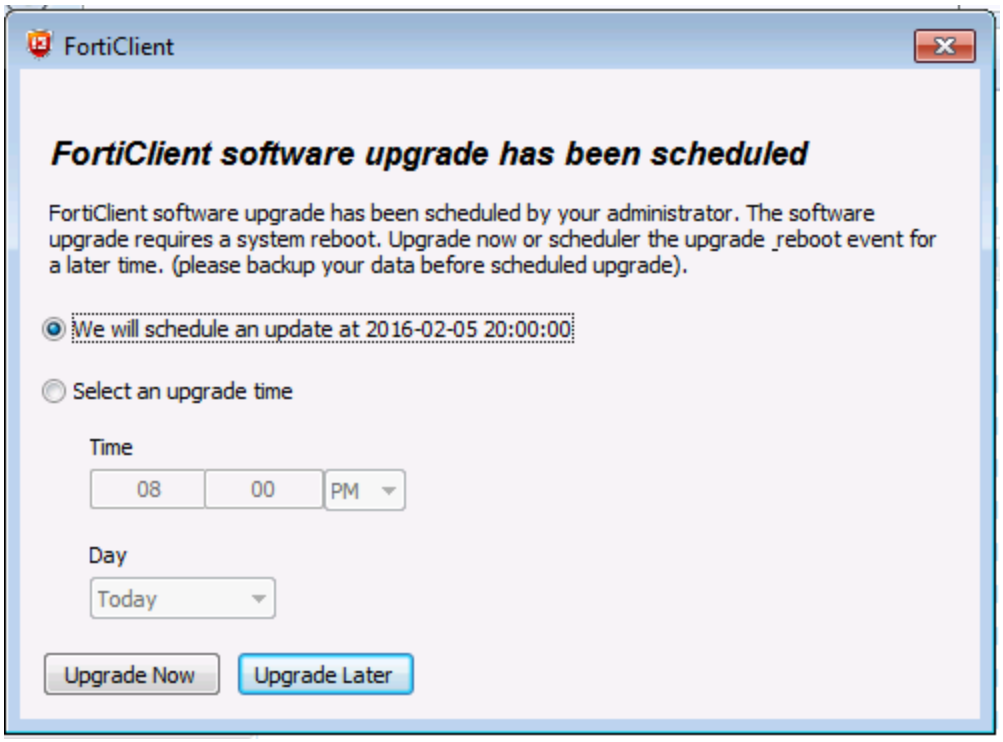
Deployment to workgroups is supported as long as the policies and credentials have the proper setup.

1. Configure the required Windows services on the AD server. Adding Endpoints on page 44.
2. Create deployment rules for the Windows Firewall. See Preparing the AD Server for Deployment on page 74.
3. Configure the Windows Firewall domain profile settings. See Preparing the AD Server for Deployment on page 74.

To deploy a FortiClient Upgrade from EMS

You can deploy a FortiClient software update from EMS. A prompt will appear in the FortiClient endpoint when an installer package is requested to be deployed. The prompt will request the user to do either of the following:

a. Upgrade Now
   If this option is selected, it will perform the upgrade and will automatically restart your computer.
b. Upgrade Later
   If this option is selected, you can indicate the time to start the upgrade. Otherwise, the default time is at 8:00PM. Your computer will automatically restart after the upgrade has finished.



c. No Option

If no option is selected, the upgrade will occur, by default at 8:00PM.

After FortiClient EMS uninstalls the previous version, it will ask if the user would like to reboot. The prompt will request the user to do either of the following:

a. Reboot Now

If this option is select, the reboot will occur immediately.

b. Reboot Later

If this option is selected, you can indicate the time to start the reboot.

c. Cancel Reboot

If this option is select, you can cancel the reboot request and reboot at your discretion.

Alerts and Log Messages

You can view alerts and log messages generated by FortiClient EMS.

Viewing alerts

You can view the alerts generated by FortiClient EMS. Examples of events that generate an alert include:

- New version of FortiClient is available
- FortiClient deployment failed
- Failure to check for signature updates
- Error encountered when downloading AD server entries
- Error encountered when scanning for local computers

A red label is associated with the *Alert* icon when new notifications are available or received. It is cleared when you view the alert.

To view alerts:

1. Click the *Alert* icon (a bell) in the toolbar. The EMS Alert Logs pane is displayed.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filter* to remove the filters.

Viewing log messages

You can view the log messages generated by FortiClient EMS.

To view log messages:

1. Go to *View* > *View Logs*. The Logs pane is displayed.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filter* to remove the filters.

Viewing raw logs

You can view the logs generated by FortiClient EMS.

To view raw logs:

1. Click the *Bell* icon in the toolbar. The EMS Alert Logs pane is displayed.
2. Click *Raw Logs*. Microsoft Windows Explorer opens with the log file selected.

Email Alert Settings

You can add an option to setup a SMTP server to enable an Alert for Endpoint Events. When an alert is triggered, an email notification will be sent. For more information, seeFortiClient EMS Settings on page 30.

FORTINET®

High Performance Network Security